

UNIVERSIDAD ABIERTA INTERAMERICANA
Facultad de Tecnología Informática



Carrera: Licenciatura en Matemática

**Descripción Matemática del Algoritmo de Shor,
para la factorización prima de números enteros
en una computadora cuántica.**

Autora: Yésica Valente
Directora: Dra. Samira Abdel Masih

***TESIS PRESENTADA PARA OPTAR AL TÍTULO DE
LICENCIADA EN MATEMÁTICA***

- Julio de 2020 -

Firmas del jurado

Agradecimientos

Quiero expresar mi más sentido agradecimiento a la Dra. Samira Abdel Masih, por su entera y maravillosa dedicación a este trabajo de tesis, así como su máximo apoyo para alcanzar esta nueva meta.

A mis padres que me dieron la vida, y me incentivaron siempre a seguir adelante, por enseñarme la importancia del estudio, el trabajo y la superación.

Agradezco a mis abuelos, que siempre esperaron este momento y hoy estarían orgullosos de mí.

A mi pareja por creer en mí, brindarme todo su amor y apoyo incondicional, y enseñarme que la perseverancia y el esfuerzo son el camino para lograr los objetivos propuestos. Y quien me alentó en cada momento de angustia y desasosiego.

A mis hermanos, sobrinos y cuñados por su cariño inmenso y continuo estímulo.

Mi agradecimiento infinito a todos mis compañeros y docentes, quienes me brindaron su ayuda, ánimos y afectos. En especial, le debo mi eterna gratitud a Hernán, mi compañero, amigo, socio, quien me acompañó a lo largo de este fascinante y complejo recorrido, no dejándome rendir nunca.

A mis amigas que muchas veces tuvieron que lamentar mi ausencia, pero que aun así siguieron junto a mí. Gracias por su apoyo moral que me permitieron permanecer con empeño, dedicación y cariño.

Y por supuesto, a mi querida Universidad Abierta Interamericana, por confiar en mí y abrirme las puertas.

Resumen

El presente trabajo analiza matemáticamente la segunda parte de la publicación desarrollada por Peter Shor en 1995, conocida como *El Algoritmo de Shor* ([1], págs. 13-20).

Dicho algoritmo, ideado para ser aplicado en una computadora cuántica, descompone en factores primos un número entero mayor que 1, en un tiempo considerablemente menor que el llevado a cabo por una computadora convencional.

El problema de la factorización es utilizado para codificar la mayoría de los mensajes secretos que se envían hoy en día.

De este modo, muchas criptografías de clave pública, tales como el sistema RSA, que se aplica en las claves bancarias online, llegarían a ser obsoletas si el *Algoritmo de Shor* fuera implementado en una computadora cuántica.

A los efectos de facilitar al lector la comprensión de los temas, éstos se ordenan y exponen de la siguiente manera:

- Introducción: Se explica someramente en qué consiste una computadora cuántica.
- Capítulo 1: Se introducen las herramientas matemáticas básicas que se utilizarán en este trabajo.
- Capítulo 2: Se define el qubit, la unidad mínima de información cuántica. Se describen además sus propiedades.
- Capítulo 3: Se definen matemáticamente los circuitos y compuertas cuánticas.
- Capítulo 4: Se desarrollan algunos algoritmos cuánticos.
- Capítulo 5: Se describe la Transformada Cuántica de Fourier.
- Capítulo 6: Se expone una aplicación de la Transformada Cuántica de Fourier, que será utilizada en el diseño del Algoritmo de Shor.
- Capítulo 7: Se analiza el Algoritmo de Shor, para la factorización de un número entero.
- Capítulo 8: Se elaboran las conclusiones.

Palabras claves:

Algoritmo de Shor, qubits, computación cuántica, Transformada Cuántica de Fourier.

Índice

Introducción

¿Qué es una computadora cuántica?	9
¿Existe en la actualidad una computadora cuántica?	9
El qubit: la unidad mínima de información en una computadora cuántica.	10
¿Cómo se codifica la información en una computadora cuántica?	10
¿Cómo funciona una computadora cuántica?	11

Capítulo 1: Nociones matemáticas previas

Los Números Complejos	12
Producto interno y tensorial de vectores	14
Transformaciones Unitarias	17
Orden de complejidad computacional de un algoritmo y funciones de orden O	18
Divisibilidad de números enteros	22
Nociones de Aritmética Modular	24
Potencia Modular	26
Algoritmo para el cálculo de Potencia Modular	27
Grupos y Subgrupos	30

Capítulo 2: Los Qubits

Sistemas formados por un qubit	37
¿Cómo medir el estado de un qubit?	39
Sistemas formados por dos qubits	40
Sistemas formados por tres qubits	44
Sistemas formados por n qubits	46
El Entrelazamiento Cuántico	51

Capítulo 3: Compuertas y circuitos cuánticos

Características de las Compuertas Cuánticas	58
Cómo modelar matemáticamente una Compuerta Cuántica	59

<i>Circuitos Cuánticos</i>	60
<i>Compuertas Cuánticas de un qubit</i>	61
<i>Principales Compuertas Cuánticas de un qubit</i>	61
<i>Las Matrices de Pauli</i>	62
<i>La Compuerta de Hadamard</i>	63
<i>La Compuerta R o de desplazamiento de fase</i>	64
<i>Compuertas Cuánticas de dos qubits</i>	67
<i>Principales Compuertas Cuánticas de dos qubits</i>	68
<i>La Compuerta Swap</i>	68
<i>La Compuerta Xor</i>	68
<i>La Compuerta $\overline{\text{Xor}}$</i>	69
<i>La Compuerta Hadamard para un sistema de dos qubits</i>	70
<i>La Compuerta f</i>	71
<i>Compuertas Cuánticas de n qubits</i>	75
<i>La Compuerta f para una función booleana de n variables</i>	75
<i>La Compuerta de Hadamard para un sistema de n qubits</i>	76

Capítulo 4: Algunos Algoritmos Cuánticos

<i>El Algoritmo de Deutch</i>	83
<i>Descripción del Algoritmo de Deutch</i>	84
<i>El Algoritmo de Deutch-Josza</i>	87
<i>Algoritmo de Deutch-Josza para funciones booleanas de dos variables</i>	88
<i>Algoritmo de Deutch-Josza para funciones booleanas de n variables</i>	91
<i>El Algoritmo de Simon</i>	93

Capítulo 5: La Transformada Cuántica de Fourier

<i>La Transformada Cuántica de Fourier de n-qubits</i>	104
<i>Representación matricial de la Transformada Cuántica de Fourier</i>	105
<i>Diseño del Circuito Cuántico para la Transformada Cuántica de Fourier</i>	106
<i>Compuertas que intervienen en el circuito de la Transformada Cuántica de Fourier</i>	106
<i>Circuito Cuántico para la Transformada Cuántica de Fourier</i>	112
<i>Circuito Cuántico de la QFT de 1-qubit</i>	112
<i>Circuito Cuántico de la QFT de 2-qubits</i>	113
<i>Circuito Cuántico de la QFT de 3-qubits</i>	114

<i>Circuito Cuántico de la QFT de n-qubits</i>	117
<i>Cantidad de Compuertas requeridas para el Circuito Cuántico de la QFT de n-qubits</i>	117

Capítulo 6: Aplicación de la Transformada Cuántica de Fourier

<i>Función Exponencial Modular</i>	119
<i>Función Periódica en $\mathbb{Z}_n$</i>	119
<i>Fracciones Continuas</i>	121
<i>Descripción del Algoritmo Cuántico para el cálculo del período de una función exponencial modular</i>	127
<i>Algoritmo de búsqueda del período P de una Función Exponencial Modular</i>	134

Capítulo 7: El Algoritmo de Shor

<i>Presentación del Problema</i>	146
<i>Hipótesis requerida para aplicar el Algoritmo de Shor</i>	146
<i>Descripción del Algoritmo de Shor</i>	146
<i>Justificación matemática del Algoritmo de Shor</i>	147
<i>Vulnerabilidad del sistema criptográfico RSA</i>	153

Capítulo 8: Conclusiones

<i>Conclusiones y Referencias</i>	154
-----------------------------------	-----

Introducción

¿Qué es una computadora cuántica?

Una computadora cuántica es un dispositivo electromagnético que utiliza ciertas propiedades de las partículas subatómicas para almacenar datos y procesar información. A diferencia de una computadora clásica, donde la unidad mínima de información es el **bit**, en una computadora cuántica la unidad mínima de información es el **qubit** o **bit cuántico**.

La idea de crear este tipo de ordenadores fue propuesta en 1959 por Richard Feynman (1918-1988), quien fuera premio Nobel de Física en 1965. Sin embargo, este proyecto fue subestimado por la comunidad científica.

Pero en la década de los 90, antes de construir la primera computadora cuántica, comenzaron a aparecer algoritmos cuánticos para ser implementados en este tipo de ordenadores. Aún así, este hecho tampoco despertó demasiado interés científico.

Hasta que en 1995 Peter Shor desarrolló un algoritmo cuántico llamado *El Algoritmo de Shor*. El mismo consistía en descomponer un número natural n como producto de números primos. Teóricamente, el tiempo que tardaba en hallar la descomposición prima del número entero era considerablemente menor al de una computadora clásica. Por ejemplo, según [15], a una computadora clásica le llevaría miles de años hallar la descomposición prima de un número entero de 300 dígitos, mientras que a un ordenador cuántico le tomaría sólo unos minutos.

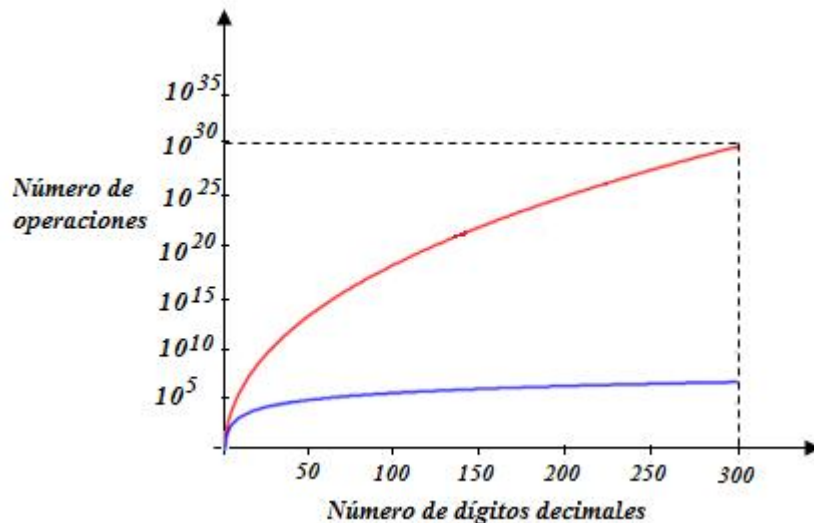


Figura 0.1: Rojo: Mejor algoritmo clásico GNFS (Criba General del Cuerpo de Números).

Azul: Algoritmo de Shor, utilizando una computadora cuántica de 10 qubits.

Este resultado sí despertó gran interés, ya que numerosas claves de seguridad bancaria se basan en la descomposición prima de un número natural y podrían fácilmente descubrirse si se aplicara el Algoritmo de Shor.

Fue a partir de entonces que muchas empresas e instituciones se preocuparon por diseñar una computadora cuántica. Entre ellas, IBM, NASA, Google y Microsoft.

¿Existe en la actualidad una computadora cuántica?

El ordenador cuántico dejó de ser sólo una teoría para convertirse en realidad en el año 1998. Fue en ese entonces que el investigador Isaac Chuang dirigió a un grupo de la Universidad de Berkeley (California) para construir la primera computadora cuántica. Ésta funcionaba con sólo un qubit.

En 2001 un grupo de IBM desarrolló una computadora cuántica capaz de controlar 7 qubits. En ese año se probó por primera vez y de manera exitosa el Algoritmo de Shor, descomponiendo el número 15 en sus factores 3 y 5.

En 2013 se diseñó un ordenador cuántico que funcionaba con 512 qubits y, según aseguran sus desarrolladores, es hasta 108 millones de veces más rápido que un ordenador tradicional.

Por el momento, empresas como Google, IBM y la NASA están implementando prototipos con la tecnología necesaria para lograr que, en unos 10 o 15 años, los ordenadores cuánticos sean una realidad cotidiana.

Según un artículo del periódico “Financial Times” [2], publicado en enero de 2020, Google afirmó haber construido la primera computadora cuántica que puede realizar cálculos que exceden la capacidad de los superordenadores más potentes de la actualidad. Más específicamente, la empresa asegura que su tecnología fue capaz de realizar en tres minutos y 20 segundos un cálculo que le tomaría al ordenador clásico más avanzado de hoy, conocido como Summit, aproximadamente 10.000 años.

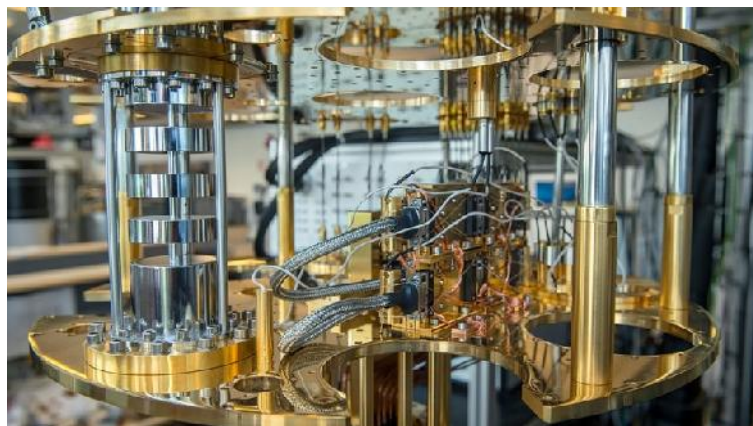


Figura 0.2: Computadora cuántica de Microsoft.

Fuente: <https://www.infobae.com/america/tecno/2019/09/20/google-asegura-haber-alcanzado-la-supremacia-cuantica/>

El qubit: la unidad mínima de información en una computadora cuántica.

Así como el bit es la unidad mínima de información en una computadora convencional, el bit cuántico o qubit es la unidad mínima de información en una computadora cuántica, y representa el estado físico de una partícula subatómica. Por lo general, y así se asumirá a lo largo de este trabajo, se considera el estado del electrón situado en la órbita más externa de un átomo. De este modo, la información se codifica sobre el estado de dicho electrón. A mayor cantidad de qubits, más rápido funcionará un ordenador cuántico.

¿Cómo se codifica la información en una computadora cuántica?

Como se mencionó anteriormente, en un qubit se almacena el estado del electrón más externo de un átomo. Pero ¿cómo se determina el estado de un electrón?

Se lo determina en base a la propiedad de “spín” que tienen las partículas subatómicas.

El **spín** (que significa giro en inglés), descubierto en 1925, es la facultad que tienen dichas partículas de poseer un *momento angular propio o intrínseco*. Para hacer una analogía con la Mecánica Clásica y por razones didácticas, se supondrá que el spin es la propiedad que tienen las partículas subatómicas de “girar” en torno a su eje. En particular, se considera el spín del electrón más externo de un átomo. Su sentido de giro queda determinado por “La Regla de la mano derecha”. Si el electrón está **spín arriba**, se encuentra en su mayor nivel de energía y se supone que está en estado **0**. Mientras que si está **spín abajo**, su nivel energético es el más bajo y se dice que está en estado **1**.

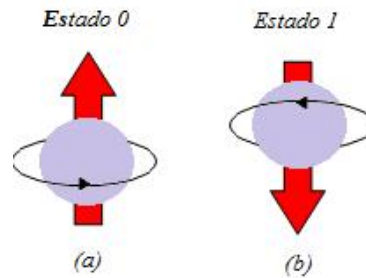


Figura 0.3: (a) Electrón girando spín arriba. En ese caso, se supone que hay almacenado un 0.
(b) Electrón girando spín abajo. Se asume que hay almacenado un 1.

Pero el electrón también puede girar en cualquier otra posición comprendida entre el estado 0 y el estado 1. Es decir, puede rotar en una posición que es combinación lineal de ambos estados.

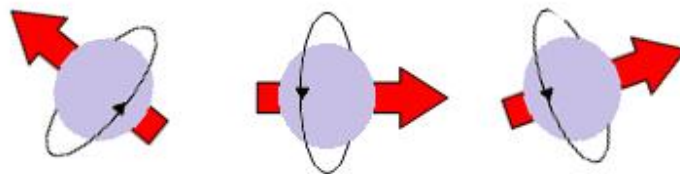


Figura 0.4: Distintas posiciones del eje de giro de un electrón

Para comprender este fenómeno, algunos comparan el spin del electrón con el movimiento de un trompo.

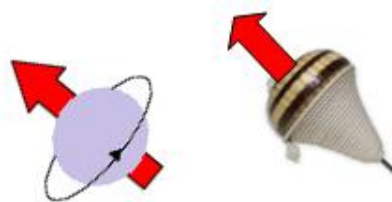


Figura 05: Analogía entre el giro de un electrón y el de un trompo.

Es por ello que, para medir la posición del eje de rotación del electrón en todas las posibles direcciones, se utiliza un par ordenado de números complejos. De este modo el qubit, que almacena la orientación del spin de un electrón, es representado mediante un vector complejo de dos componentes. Por ejemplo, si el electrón está spín arriba, el valor del qubit es $(1,0)^T$, y se lo simboliza por $|0\rangle$. Mientras que, si está spín abajo, su valor es $(0,1)^T$ y se lo representa por $|1\rangle$.

En caso de que el eje de rotación tome una posición distinta a las de spín arriba o spín abajo, se supone que el electrón está en ambos estados al mismo tiempo.

Por esta razón se afirma que un qubit puede adoptar simultáneamente los estados 0 y 1. Este hecho es lo que permite, a una computadora cuántica, procesar varios datos simultáneamente.

¿Cómo funciona una computadora cuántica?

En un procesador cuántico no se utilizan ni monitores, ni discos duros, ni ningún tipo de hardware tal como se conoce en el ámbito de la informática actual.

Todo sucede en la unidad de procesamiento que debe permanecer en unas condiciones de absoluto aislamiento, ya que los estados cuánticos del átomo son extremadamente frágiles y la superposición de los estados que se produce durante los procesos de cálculo, puede perturbarse.

Así, la superposición podría verse afectada ante el contacto con un campo electromagnético o la más mínima vibración o fluctuación de la temperatura.

Esta eventual alteración del estado cuántico del átomo provocaría errores de cálculo. Por esta razón, los procesadores en los que se encuentran los qubits deben enfriarse y mantenerse cercanos al cero absoluto (- 273.15 grados Celcius).

Los estados de cada qubit se observan mediante mediciones con láser, de las que se extraen los resultados de los cálculos y se procesan con ordenadores normales.

¿Qué desafíos se plantean en esta tesis?

En este trabajo se intentará mostrar cómo la Computación Cuántica y en particular la Algoritmia Cuántica, una ciencia que se encuentra en sus inicios, puede ser entendida sin dificultad si se la modela matemáticamente aplicando conocimientos básicos de Números Complejos, Álgebra Lineal y Probabilidad.

La escasa bibliografía que existe en relación a ejemplos que ilustren cada definición, como así también el funcionamiento de un algoritmo cuántico, motivará a utilizar esta metodología para facilitar al lector la comprensión de los temas.

Capítulo 1

Nociones matemáticas previas

En este capítulo se expondrán los principales conceptos matemáticos que se utilizarán a lo largo de este trabajo. Primeramente se presentarán a los números complejos, para luego desarrollar el producto interno y el producto tensorial de vectores. Finalmente se introducirán las nociones de Aritmética Modular y sus propiedades básicas.

Los números complejos

Definición 1.1 : Un número complejo z es una expresión de la forma

$$z = a + i b$$

Donde a y b son números reales, $i = \sqrt{-1}$. En este caso,

$$a = \text{Re}(z) \text{ (parte real de } z \text{)} \quad b = \text{Im}(z) \text{ (parte imaginaria de } z \text{)}$$

Representación gráfica de los números complejos

Los números complejos se representan en el “Plano Complejo” del siguiente modo:

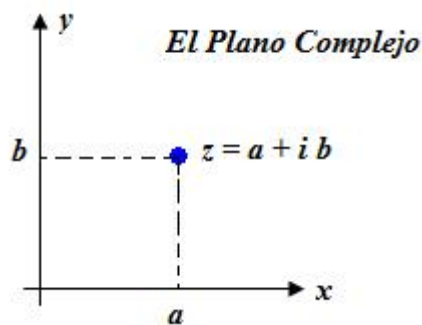


Figura 1.1: Representación gráfica de un número complejo

Otra representación posible de z en este plano es en forma de vector, con origen en el origen de coordenadas y extremo en el punto z .

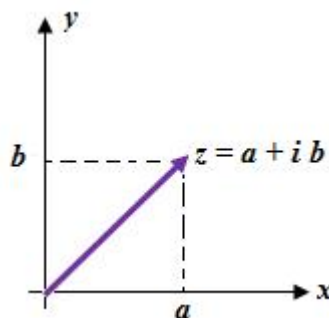


Figura 1.2: Representación vectorial de un número complejo.

Igualdad de números complejos

Dados dos números complejos $z_1 = a_1 + i b_1 \wedge z_2 = a_2 + i b_2$ entonces

$$z_1 = z_2 \Leftrightarrow a_1 = a_2 \wedge b_1 = b_2$$

Módulo o valor absoluto de un número complejo

Si $z = a + i b$, el módulo de z es

$$|z| = \sqrt{a^2 + b^2}.$$

Dicho número representa la distancia de z al origen de coordenadas.

El complejo conjugado

Si $z = a + i b$, el complejo conjugado de z , simbolizado por $\bar{z}$, es

$$\bar{z} = a - i b.$$

Forma exponencial de un número complejo.

Si $z = a + i b$ es un complejo no nulo, podemos definir sus componentes usando coordenadas polares:

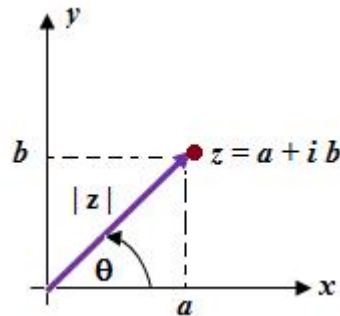


Figura 1.3: Representación de un número complejo aplicando coordenadas polares.

Donde

$$|z| = \sqrt{a^2 + b^2}$$

$\bar{\theta}$ = ángulo, expresado en radianes, entre el vector de componentes (a, b) y el semieje x positivo, medido en sentido antihorario ($0 \leq \theta < 2\pi$).

Por lo tanto, si $z \neq 0$ entonces

$$\begin{cases} \cos(\bar{\theta}) = \frac{a}{|z|} \\ \sin(\bar{\theta}) = \frac{b}{|z|} \end{cases} \Rightarrow \begin{cases} a = |z| \cos(\bar{\theta}) \\ b = |z| \sin(\bar{\theta}) \end{cases}$$

Luego, todo complejo no nulo puede expresarse como

$$z = a + i b = |z| \cos(\bar{\theta}) + i |z| \sin(\bar{\theta}) = |z| (\cos(\bar{\theta}) + i \sin(\bar{\theta})).$$

Teniendo en cuenta la Fórmula de Euler:

$$e^{i\bar{\theta}} = (\cos(\bar{\theta}) + i \sin(\bar{\theta}))$$

Surge la siguiente:

Definición 1.2 : Forma exponencial de un número complejo

Dado un número complejo $z = a + i b$, su representación en forma exponencial es

$$z = |z| e^{i\varphi}$$

Donde

$$|z| = \sqrt{a^2 + b^2}$$

φ = ángulo (en radianes) entre el vector de componentes (a, b) y el semieje x positivo.

Igualdad de números complejos expresados en forma exponencial

Dados dos números complejos $z_1 \wedge z_2$ expresados en forma exponencial, es decir,

$$z_1 = |z_1| e^{i\varphi_1} \wedge z_2 = |z_2| e^{i\varphi_2} \text{ entonces}$$

$$z_1 = z_2 \Leftrightarrow |z_1| = |z_2| \wedge \varphi_1 = \varphi_2 + 2k\pi, \text{ con } k \in \mathbb{Z}$$

Producto interno y tensorial de vectores**Definición 1.3: Producto interno de vectores**

Sea F el cuerpo de los números reales o de los complejos y V un espacio vectorial sobre F . Un “Producto interno” sobre V es una función que asigna, a cada par ordenado de vectores (v, w) , un escalar $\langle v, w \rangle$ de F de modo tal que $\forall v, w, u \in V$ y $\forall \alpha \in F$, se verifican las siguientes propiedades:

- 1) $\langle v + w, u \rangle = \langle v, u \rangle + \langle w, u \rangle$
- 2) $\langle \alpha v, w \rangle = \alpha \langle v, w \rangle$
- 3) $\langle v, w \rangle = \overline{\langle w, v \rangle}$ donde la barra indica conjugación compleja.
- 4) $\langle v, v \rangle \geq 0 \quad \forall v \in V$
- 5) $\langle v, v \rangle > 0$ si $v \neq 0$ y donde 0 representa el vector nulo.

Ejemplo 1.4

Si $v = (v_1, v_2, \dots, v_n)^T$ y $w = (w_1, w_2, \dots, w_n)^T$ son vectores en $\mathbb{C}^n$ entonces

$$\langle v, w \rangle = \sum_{i=1}^n v_i \overline{w_i}$$

Es un producto interno, llamado “el producto interno canónico”.

La siguiente Proposición, que será útil para las demostraciones posteriores, es una consecuencia inmediata de las propiedades del producto interno:

Proposición 1.5

Si $v, w \in V$ y $\alpha \in F$ entonces $\langle v, \alpha w \rangle = \overline{\alpha} \langle v, w \rangle$

Demostración

Aplicando las Propiedades 3) y 4) del producto interno y la propiedad de la conjugación del producto de dos números complejos, resulta

$$\langle v, \alpha w \rangle = \overline{\langle \alpha w, v \rangle} = \overline{\alpha \langle w, v \rangle} = \overline{\alpha} \overline{\langle w, v \rangle} = \overline{\alpha} \langle v, w \rangle \quad \blacksquare$$

En todo espacio vectorial con producto interno queda definida la “norma o módulo de un vector” del siguiente modo:

Definición 1.6: Norma o módulo de un vector

Dado un espacio vectorial V con producto interno, la norma o módulo de un vector $v \in V$ es

$$\|v\| = \sqrt{\langle v, v \rangle}$$

Definición 1.7: Producto tensorial de vectores

Sean $V = F^n$ y $W = F^m$ dos espacios vectoriales de dimensión n y m respectivamente, con $F = \mathbb{R}$ ó $\mathbb{C}$.

Si $v = (v_1, v_2, \dots, v_n)^T$ y $w = (w_1, w_2, \dots, w_m)^T$ entonces el producto tensorial de v con w , simbolizado por $v \otimes w$, se lo define así:

$$v \otimes w = \begin{pmatrix} v_1 w \\ v_2 w \\ \vdots \\ v_n w \end{pmatrix} = \begin{pmatrix} v_1 \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix} \\ v_2 \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix} \\ \vdots \\ v_n \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_m \end{pmatrix} \\ \begin{pmatrix} v_2 w_1 \\ v_2 w_2 \\ \vdots \\ v_2 w_m \end{pmatrix} \\ \vdots \\ \begin{pmatrix} v_n w_1 \\ v_n w_2 \\ \vdots \\ v_n w_m \end{pmatrix} \end{pmatrix}$$

Claramente se puede verificar que el producto tensorial no es conmutativo. Es decir,

$$v \otimes w \neq w \otimes v$$

El siguiente ejemplo muestra cómo se calcula un producto tensorial.

Ejemplo 1.8

Si $v = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ y $w = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}$, calcular $v \otimes w$ y $w \otimes v$.

Solución

$$v \otimes w = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \otimes \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \\ 3 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 8 \\ 10 \\ 12 \end{pmatrix} \\ \begin{pmatrix} 12 \\ 15 \\ 18 \end{pmatrix} \end{pmatrix}$$

Por otro lado,

$$w \otimes v = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 4 \begin{pmatrix} 2 \\ 3 \end{pmatrix} \\ 5 \begin{pmatrix} 2 \\ 3 \end{pmatrix} \\ 6 \begin{pmatrix} 2 \\ 3 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 8 \\ 12 \end{pmatrix} \\ \begin{pmatrix} 10 \\ 15 \end{pmatrix} \\ \begin{pmatrix} 12 \\ 18 \end{pmatrix} \end{pmatrix}$$

Las propiedades básicas del producto tensorial se enumeran en la siguiente Proposición:

Proposición 1.9

- 1) Si $u \in F^n$ y $v, w \in F^m$ entonces $u \otimes (v + w) = (u \otimes v) + (u \otimes w)$
- 2) Si $u, v \in F^n$ y $w \in F^m$ entonces $(u + v) \otimes w = (u \otimes w) + (v \otimes w)$
- 3) Si $u \in F^n$, $v \in F^m$ y $\alpha \in \mathbb{C}$ entonces

$$\begin{aligned} (\alpha u) \otimes v &= \alpha (u \otimes v) \\ u \otimes (\alpha v) &= \alpha (u \otimes v) \end{aligned}$$

- 4) Si $u \in F^n$, $v \in F^m$ y $\alpha > 0$ entonces $\alpha (u \otimes v) = (\sqrt{\alpha} u) \otimes (\sqrt{\alpha} v)$

Demostración

Véase [3], pág.16 ■

Observación 1.10

A fin de simplificar la notación, se eliminarán los paréntesis internos que figuran en el resultado de un producto tensorial.

Es decir, si $v = (v_1, v_2, \dots, v_n)^T$ y $w = (w_1, w_2, \dots, w_m)^T$ entonces

$$v \otimes w = \begin{pmatrix} \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_m \end{pmatrix} \\ \begin{pmatrix} v_2 w_1 \\ v_2 w_2 \\ \vdots \\ v_2 w_m \end{pmatrix} \\ \vdots \\ \begin{pmatrix} v_n w_1 \\ v_n w_2 \\ \vdots \\ v_n w_m \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_m \\ v_2 w_1 \\ v_2 w_2 \\ \vdots \\ v_2 w_m \\ \vdots \\ v_n w_1 \\ v_n w_2 \\ \vdots \\ v_n w_m \end{pmatrix}$$

De este modo, si $v \in F^n$ y $w \in F^m$ el producto tensorial $v \otimes w$ será identificado mediante un vector en F^{nm} .

Ejemplo 1.11

Si $v = \begin{pmatrix} 6 \\ 2 \end{pmatrix}$ y $w = \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}$ entonces

$$v \otimes w = \begin{pmatrix} 6 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 6 \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} \\ 2 \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 18 \\ 24 \\ 30 \end{pmatrix} \\ \begin{pmatrix} 6 \\ 8 \\ 10 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 18 \\ 24 \\ 30 \\ 6 \\ 8 \\ 10 \end{pmatrix}$$

De este modo, $v \otimes w$ es identificado como un vector en $\mathfrak{R}^6$.

Transformaciones unitarias

Las transformaciones lineales, y en particular las unitarias, desempeñan un rol importante en Computación Cuántica debido a que las compuertas cuánticas se modelan matemáticamente en términos de estas transformaciones, como se verá en el Capítulo 3. En esta sección se recordará su definición:

Definición 1.12: Transformación lineal

Sean V y W dos espacios vectoriales sobre el mismo cuerpo K . Una transformación lineal de V en W es una función $T: V \rightarrow W$ que verifica:

- 1) $T(u + v) = T(u) + T(v)$
- 2) $T(k v) = k T(v)$, $\forall u, v \in V \wedge \forall k \in K$

Definición 1.13: Transformación unitaria

Sea V un espacio vectorial con producto interno. Una transformación lineal $T: V \rightarrow V$ es unitaria si :

$$\langle T(u), T(v) \rangle = \langle u, v \rangle \quad \forall u, v \in V$$

Ejemplo 1.14

Sea el espacio vectorial $V = \mathbb{C}^2$ definido sobre el cuerpo $K = \mathbb{C}$ y con el producto interno canónico. Sea $T: \mathbb{C}^2 \rightarrow \mathbb{C}^2$ definida por $T(x, y) = (y, -x)$, con $x, y \in \mathbb{C}$.

- Probar que T es una transformación unitaria.
- Hallar la matriz asociada a la transformación T .

Solución

a) T es una transformación lineal pues:

Sean $u, v \in \mathbb{C}^2$ y $k \in \mathbb{C}$ entonces $u = (x_1, y_1)$, $v = (x_2, y_2)$ con $x_1, y_1, x_2, y_2 \in \mathbb{C}$.
Luego

$$1) T(u+v) = T(x_1+x_2, y_1+y_2) = (y_1+y_2, -(x_1+x_2)) = (y_1, -x_1) + (y_2, -x_2) = \\ = T(x_1, y_1) + T(x_2, y_2) = T(u) + T(v)$$

$$2) T(u+kv) = T(kv) = T(kx_2, ky_2) = (ky_2, -kx_2) = k(y_2, -x_2) = kT(v)$$

T es unitaria pues

$$\langle T(u), T(v) \rangle = \langle (y_1, -x_1), (y_2, -x_2) \rangle = y_1 \overline{y_2} + (-x_1)(\overline{-x_2}) = y_1 \overline{y_2} + (-x_1)(-\overline{x_2}) = \\ = y_1 \overline{y_2} + x_1 \overline{x_2} = \langle (x_1, y_1), (x_2, y_2) \rangle = \langle u, v \rangle.$$

b) Sea $\{(1, 0), (0, 1)\}$ una base de $\mathbb{C}^2$. Para hallar la matriz asociada a la transformación, se valúa T en cada elemento de la base:

$T(1, 0) = (0, -1)$; $T(0, 1) = (1, 0)$. Luego, la matriz U asociada a T es

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Orden de complejidad computacional de un algoritmo y funciones de orden O

La resolución práctica de un problema exige por una parte un algoritmo o método de resolución y por otra parte, para que pueda ser implementado una computadora, su programación o codificación.

Desde el punto de vista de la Ingeniería y de la Informática, lo que preocupa son los recursos físicos necesarios para que un algoritmo pueda ejecutarse. De todos ellos, los más importantes son dos: **el tiempo de ejecución** y **la cantidad de memoria** que requiere el algoritmo. Estos dos parámetros definen básicamente el orden de complejidad computacional de un algoritmo y, para medirlos, se utiliza el concepto de “funciones de orden O ”. Su definición se da a continuación:

Definición 1.15: Funciones de orden O

Sea $f: \mathbb{N} \rightarrow [0, +\infty)$. El conjunto de funciones de orden O de f , simbolizado por $O(f)$ es

$$O(f) = \left\{ g: \mathbb{N} \rightarrow \mathbb{R} \text{ tal que } \exists k > 0 \wedge n_0 \in \mathbb{N} / |g(n)| \leq k f(n) \forall n \geq n_0 \right\}$$

Así, una función $g: \mathbb{N} \rightarrow \mathbb{R}$ se dice que es $O(f)$ si $g \in O(f)$.

Ejemplo 1.16

Si $g(n) = 2n^4 + 6n^3$ y $f(n) = 5n^4 + 2n$, probar que g es $O(f)$.

Solución

Se observa que, $\forall n \geq 1$ se verifica que $f(n) = 5n^4 + 2n \geq 5n^4$.

Por lo tanto

$$\frac{|g(n)|}{f(n)} = \frac{g(n)}{f(n)} = \frac{2n^4 + 6n^3}{5n^4 + 2n} \leq \frac{2n^4 + 6n^3}{5n^4} = \frac{2}{5} + \frac{6n^3}{5n^4} = \frac{2}{5} + \frac{6}{5n} \leq \frac{2}{5} + \frac{6}{5} = \frac{8}{5}$$

Por lo tanto, tomando $n_0 = 1$ y $k = \frac{8}{5}$ se verifica que $|g(n)| \leq k f(n) \forall n \geq n_0$. En consecuencia, $g \in O(f)$ ■

Proposición 1.17

1) Si $\lim_{n \rightarrow \infty} \frac{|g(n)|}{f(n)} \leq M$ para alguna constante M entonces $g \in O(f)$.

2) Si $f_1 \in O(g)$ y $f_2 \in O(h) \Rightarrow f_1 \cdot f_2 \in O(g \cdot h)$

Demostración

Véase [3], pág.18 ■

Observación 1.18

1) A menudo, para enfatizar que las funciones f y g tienen por variable independiente a un número natural n , en lugar de afirmar que g es $O(f)$ se suele decir que $g(n)$ es $O(f(n))$. Esta notación es la que se aplicará en adelante.

2) Una ecuación de la forma

$$g(n) = h(n) + O(f(n))$$

Significa que $g(n) - h(n) = O(f(n))$. Es decir, que

$$|g(n) - h(n)| \leq k f(n)$$

Para alguna constante $k > 0$ y $\forall n \geq n_0$.

A continuación se definirá el orden de complejidad computacional de un algoritmo, concepto que es muy utilizado para comparar la eficiencia de distintos algoritmos que se plantean.

Definición 1.19: Orden de complejidad computacional de un algoritmo

Se dice el orden de complejidad de un algoritmo es $O(f(n))$ donde $f: \mathbb{N} \rightarrow [0, +\infty)$ si el tiempo de ejecución o la cantidad de memoria requerida para ejecutar el algoritmo se expresa mediante una función $g(n)$, con $g(n) \in O(f(n))$

En este caso, “ n ” puede representar la longitud de un vector, el orden de una matriz, el número de registros de una base de datos, etc. Por otro lado, la definición de $O(f)$ permite asegurar que, a partir de cierto “ n ” en adelante, el tiempo de ejecución de un algoritmo o la cantidad de memoria requerida nunca será superior a $f(n)$. Es decir que, si “ n ” es suficientemente grande, y salvo una constante multiplicativa “ k ”, $f(n)$ es una cota superior de $g(n)$. Además, el hecho de indicar, en la definición de $O(f)$, que “ n ” sea mayor que cierto valor n_0 se debe a que la eficiencia de un algoritmo se mide para valores de “ n ” muy grandes. Ya que, casi siempre, los problemas pequeños se pueden resolver de cualquier manera, apareciendo las limitaciones al atacar problemas grandes. Por lo general, la función $f(n)$ se escoge de modo tal que sea lo más sencilla posible. Esto da lugar a la siguiente definición.

Definición 1.20: Clasificación del orden de complejidad de un algoritmo

- 1) Si $f(n) = \log(n)$ se dice que el algoritmo es de orden logarítmico.
- 2) Si $f(n) = n^p$ con $p \in \mathbb{N}$ se dice que el algoritmo es de orden polinomial.
En este caso, se lo considera **eficiente**.
- 3) Si $f(n) = a^n$ con $a > 1$, se dice que el algoritmo es de orden exponencial o No Polinomial (NP).
En este caso, se lo considera **ineficiente**.

Los algoritmos de **orden logarítmico** son los ideales, ya que el tiempo que demandan para procesar los datos se reduce considerablemente.

Los de **orden polinomial** se enfrentan a una dificultad a medida que “ p ” crece. Mientras menor sea el valor de “ p ”, más eficiente será el algoritmo. Complejidades del orden $O(n^2)$ y $O(n^3)$ suelen ser efectivamente abordables, y prácticamente nadie acepta algoritmos de orden $O(n^{100})$.

Los algoritmos de **orden exponencial** suelen ser intratables y sólo son aplicables a problemas con valores de “ n ” pequeños.

A la vista de lo expuesto, se comprende que los programadores busquen algoritmos de orden polinomial, ya que es un golpe de suerte encontrar de orden logarítmico.

Se finalizará esta sección mostrando un ejemplo que ilustrará cómo clasificar el orden de complejidad de un algoritmo.

Ejemplo 1.21

Sean $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$ y $B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}$ dos matrices en $\mathfrak{R}^{n \times n}$.

Se tiene un ordenador que tarda T unidades de tiempo para efectuar una operación aritmética (suma, resta, multiplicación o división). Probar que el tiempo requerido para efectuar el producto matricial $A \cdot B$ es $O(n^3)$.

Solución

El producto escalar matricial $A \cdot B$ es una matriz en $\mathfrak{R}^{n \times n}$ cuyos coeficientes son

$$(A \cdot B)_{ij} = \sum_{k=1}^n a_{ik} \cdot b_{kj}, \quad \forall i, j = 1, \dots, n$$

Para efectuar este cálculo se necesitan, para cada i y para cada j , n multiplicaciones y $(n-1)$ sumas. Por lo tanto, para cada i y para cada j , son necesarias $n + (n-1) = 2n - 1$ operaciones aritméticas. Luego, el total de operaciones aritméticas necesarias para calcular $A \cdot B$ es

$$\sum_{i=1}^n \sum_{j=1}^n (2n - 1) = \sum_{i=1}^n n(2n - 1) = n n(2n - 1) = 2n^3 - n^2$$

En consecuencia, el ordenador tardará $(2n^3 - n^2)T$ unidades de tiempo para efectuar el producto matricial. En este caso, $g(n) = (2n^3 - n^2)T$. Si se define $f(n) = n^3$ entonces, del inciso 1) de la Proposición 1.17 resulta

$$\lim_{n \rightarrow \infty} \frac{|g(n)|}{f(n)} = \lim_{n \rightarrow \infty} \frac{|(2n^3 - n^2)T|}{n^3} = \lim_{n \rightarrow \infty} \frac{(2n^3 - n^2)T}{n^3} = 2T$$

Tomando $M = 2T$ se obtiene que $g \in O(n^3)$ y en consecuencia, el tiempo requerido para efectuar el producto matricial es $O(n^3)$, con lo cual es de orden polinomial.

Divisibilidad de números enteros

En esta sección se enunciarán algunas propiedades básicas de los números enteros, que se aplicarán en los capítulos subsiguientes.

Teorema 1.22: Algoritmo de la División Entera

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen dos números enteros q y r , llamados cociente y resto, que verifican:

$$1) a = b q + r \quad 2) 0 \leq r < |b|$$

Demostración

Véase [11]. ■

Definición 1.23: Divisibilidad

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Se dice que “ b divide a a ” y se escribe $b \mid a$ si $a = k b$ para algún $k \in \mathbb{Z}$ o equivalentemente, si al dividir a por b , el resto da 0.

Definición 1.24: Máximo Común Divisor

Sean $a, b \in \mathbb{Z}$ tales que no son simultáneamente nulos. Se dice que d es el máximo común divisor entre a y b si verifica:

1) $d > 0$

2) $d \mid a \wedge d \mid b$

3) Si existe $c \in \mathbb{Z}$ tal que $c \mid a \wedge c \mid b \Rightarrow c \mid d$

Notación 1.24: Al máximo común divisor entre a y b se lo simbolizará por $\text{mcd}(a, b)$.

El Algoritmo de Euclides brinda una manera sencilla y eficiente, desde el punto de vista computacional, de calcular el máximo común divisor. Dicho algoritmo se describe a continuación.

Algoritmo 1.25: El Algoritmo de Euclides

Sean $a, b \in \mathbb{Z}$ con $b > 0$. Aplicando reiteradamente el Algoritmo de la División Entera, se tienen las siguientes ecuaciones recursivas:

$$a = b \cdot q_1 + r_1, \quad 0 \leq r_1 < b$$

$$b = r_1 \cdot q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3, \quad 0 \leq r_3 < r_2$$

.....

Como cada resto verifica que $0 \leq r_i < r_{i-1} \quad \forall i$, el proceso es finito. El último paso es:

$$r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}, \quad r_{n+1} = 0.$$

Por lo tanto, $\text{mcd}(a, b) = r_n$

Ejemplo 1.26

Hallar el máximo común divisor entre 80 y 30.

Solución

Se elabora el siguiente cuadro:

Dividendo	Divisor	Cociente	Resto
80	30	2	20
30	20	1	10
20	10	2	0

Por lo tanto, $\text{mcd}(a, b) = 10$.

Teorema 1.27

Sean $a, b \in \mathbb{Z}$ tales que no son simultáneamente nulos.

Si $d = \text{mcd}(a, b) \Rightarrow \exists p, q \in \mathbb{Z}$ tales que $d = p \cdot a + q \cdot b$

Demostración

Véase [11]. ■

Teorema 1.28: Teorema Fundamental de la Aritmética

Todo número entero $n > 1$ puede ser representado exactamente, salvo el orden, de una única manera, como producto de potencias de números primos. Es decir,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i}$$

Donde

$p_1 < p_2 < \dots < p_k$ son números primos

α_i son enteros positivos $\forall i = 1, 2, \dots, k$

Demostración

Véase [11]. ■

Nociones de Aritmética Modular

Definición 1.29: Congruencia

Dado un número natural $n > 1$ y dos números enteros a y b , se dice que a es congruente con b módulo n , y se escribe

$$a \equiv b \pmod{n}$$

Si

$$n \mid (a - b)$$

La siguiente Proposición, cuya demostración se puede encontrar en cualquier bibliografía de Aritmética Modular, enuncia las propiedades básicas de la congruencia:

Proposición 1.30

- 1) $a \equiv b \pmod{n} \Leftrightarrow a$ y b tienen el mismo resto en la división entera por n .
- 2) $a \equiv 0 \pmod{n} \Leftrightarrow n \mid a$
- 3) $a \equiv 0 \pmod{2} \Leftrightarrow a$ es par.
- 4) Si $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a c \equiv b d \pmod{n}$
- 5) Si $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$
- 6) $a \equiv b \pmod{n} \wedge c \neq 0 \Rightarrow a c \equiv b c \pmod{n}$
- 7) $a \equiv b \pmod{n} \wedge k \in \mathbb{N} \Rightarrow a^k \equiv b^k \pmod{n}$
- 8) $a \equiv r_a \pmod{n}$ donde r_a es el resto de la división entera de a por n .
- 9) $a \equiv n + a \pmod{n}$

Definición 1.31: Suma modular

Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Entonces

$a + b = c \pmod{n} \Leftrightarrow c$ es el resto de dividir $(a + b)$ por n .

Definición 1.32: Suma "módulo 2"

Si $n = 2$, la suma modular se la representa mediante el símbolo $\oplus$. Es decir,

$a \oplus b = c \Leftrightarrow c$ es el resto de dividir $(a + b)$ por 2.

Definición 1.33: Producto modular

Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Entonces

$a \cdot b = c \pmod{n} \Leftrightarrow c$ es el resto de dividir $(a \cdot b)$ por n .

Definición 1.34: Inverso multiplicativo modular

Dado $a \in \mathbb{Z}$ y $n \in \mathbb{N}$, se dice que a tiene inverso multiplicativo $(\text{mod } n)$ si $\exists b \in \mathbb{Z}$ tal que $a \cdot b \equiv 1 \pmod{n}$

De la Proposición 1.30 inciso 8), se sabe que si $a \in \mathbb{Z}$ y n es un natural mayor que 1, entonces $a \equiv r_a \pmod{n}$, donde r_a es el resto de la división entera de a por n . Esto permite clasificar a los números enteros según el resto de su división entera por n . Como los posibles restos son $0, 1, \dots, n-1$, surge la siguiente:

Definición 1.35: El conjunto $\mathbb{Z}_n$

Si n es un número natural mayor que 1, el conjunto $\mathbb{Z}_n$ es

$$\mathbb{Z}_n = \{ 0, 1, 2, \dots, n-1 \}.$$

A dicho conjunto se le definirán ciertas operaciones, a fin de dotarlo de una estructura algebraica conveniente.

Definición 1.36: Suma y producto en $\mathbb{Z}_n$

Sean $a, b, c \in \mathbb{Z}_n$ Entonces

- 1) $a + b = c$ en $\mathbb{Z}_n \Leftrightarrow c$ es el resto de la división entera de $(a+b)$ por n .
- 2) $a \cdot b = c$ en $\mathbb{Z}_n \Leftrightarrow c$ es el resto de la división entera de $(a \cdot b)$ por n .

Definición 1.37: Elementos neutros para la suma y la multiplicación en $\mathbb{Z}_n$

- 1) El neutro para la suma es 0 pues $a + 0 \equiv a \pmod{n} \forall a \in \mathbb{Z}_n$.
- 2) El neutro para el producto es 1 pues $a \cdot 1 \equiv a \pmod{n} \forall a \in \mathbb{Z}_n$.

Definición 1.38: El opuesto en $\mathbb{Z}_n$

Dado $a \in \mathbb{Z}_n$, el opuesto de a es un número $b \in \mathbb{Z}_n$ tal que $a + b = 0$ en $\mathbb{Z}_n$.
En este caso, el opuesto de a es $(n - a)$.

Definición 1.39: El inverso en $\mathbb{Z}_n$

Dado $a \in \mathbb{Z}_n$, el inverso de a es un número $b \in \mathbb{Z}_n$ tal que $a \cdot b = 1$ en $\mathbb{Z}_n$.

Notación 1.40: al inverso de $a \in \mathbb{Z}_n$ se simbolizará por a^{-1} , mientras que al opuesto de a se lo representará por $-a$.

El siguiente teorema indica en qué casos un elemento de $\mathbb{Z}_n$ es invertible:

Teorema 1.41: Teorema de Invertibilidad en $\mathbb{Z}_n$

Un elemento $a \in \mathbb{Z}_n$ es invertible $\Leftrightarrow \text{mcd}(a, n) = 1$

Demostración

Véase [4], pág. 21 ■

Corolario 1.42

Si n es primo entonces todo elemento no nulo de $\mathbb{Z}_n$ es invertible

Demostración

Véase [4], pág. 22 ■

Ejemplo 1.43

Todo elemento de $\mathbb{Z}_{11}$ es invertible pues 11 es un número primo. Por otro lado, si $a=5$ y $b=8$ entonces

$a + b = 5 + 8 = 13 \equiv 2 \pmod{11}$ pues el resto de dividir $a + b$ por 11 es 2.

$a \cdot b = 5 \cdot 8 = 40 \equiv 7 \pmod{11}$ pues el resto de dividir $a \cdot b$ por 11 es 7.

Potencia modular

La potencia modular consiste en calcular

$$a^k \pmod{n}$$

Donde $k, a, n \in \mathbb{N}$.

Si “ a ” fuera un número entero muy grande y se intentara hallar $a^k \pmod{n}$ calculando primeramente a^k y luego efectuando su división entera por n para determinar el resto, resultaría bastante tedioso e ineficiente. Inclusive, si se hiciera este cálculo en un computador, se correría el riesgo de producirse *overflow* o *desbordamiento*. Este hecho ocurre cuando un cálculo con números enteros produce un resultado mayor a lo que puede almacenar el registro de un ordenador.

Por esta razón se presentará el siguiente algoritmo que podrá ser implementado en una computadora clásica y que permitirá calcular $a^k \pmod{n}$ de un modo más sencillo y eficiente. Como se verá en el Capítulo 7, el cálculo de una potencia modular desempeñará un rol importante en el Algoritmo de Shor.

Algoritmo para el cálculo de la potencia modular

El procedimiento para calcular $a^k \pmod{n}$ se basa en el siguiente hecho:

Si se efectúa la división entera de k por 2, se obtiene

$$k = 2 \left\lfloor \frac{k}{2} \right\rfloor + r$$

Donde

$$\left\lfloor \frac{k}{2} \right\rfloor : \text{Parte entera de } \frac{k}{2}.$$

r : Resto de la división ($0 \leq r \leq 1$).

En consecuencia,

$$a^k = a^{2 \left\lfloor \frac{k}{2} \right\rfloor + r} = \left(a^2\right)^{\left\lfloor \frac{k}{2} \right\rfloor} \cdot a^r$$

Esta expresión permite generar las siguientes sucesiones:

$$\{a_0, a_1, a_2, \dots\}, \{k_0, k_1, k_2, \dots\}, \{c_0, c_1, c_2, \dots\}, \{r_0, r_1, r_2, \dots\}$$

Donde

$$\begin{cases} a_0 = a \\ k_0 = k \\ c_0 = 1 \\ r_0 = r \end{cases}$$

Los demás términos de las sucesiones se definen del siguiente modo, aplicando las propiedades de congruencia enunciadas en los incisos 1), 4) y 7) de la Proposición 1.30:

$$a^k = a^{2 \left\lfloor \frac{k}{2} \right\rfloor + r_0} = \left(a^2\right)^{\left\lfloor \frac{k}{2} \right\rfloor} \cdot a^{r_0} \equiv a_1^{k_1} \cdot c_1 = \left(a_1^2\right)^{\left\lfloor \frac{k_1}{2} \right\rfloor} \cdot a_1^{r_1} \cdot c_1 \equiv a_2^{k_2} \cdot c_2 = \dots$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \begin{cases} a_1 \equiv a^2 \pmod{n} \\ k_1 = \left\lfloor \frac{k}{2} \right\rfloor \\ c_1 \equiv a^{r_0} = a^{r_0} \cdot c_0 \pmod{n} \end{cases} & & \begin{cases} a_2 \equiv a_1^2 \pmod{n} \\ k_2 = \left\lfloor \frac{k_1}{2} \right\rfloor \\ c_2 \equiv a_1^{r_1} \cdot c_1 \pmod{n} \end{cases} \end{array}$$

El proceso sigue hasta que $k_i \leq 1$ para algún i . El pseudocódigo del algoritmo se muestra a continuación:

Algoritmo para calcular $a^k \pmod n$

$$a_0 = a, k_0 = k, c_0 = 1, i = 1$$

Mientras $k_{i-1} > 1$ hacer:

$$a_i \equiv a_{i-1}^2 \pmod n$$

Si k_{i-1} es par entonces

$$c_i = c_{i-1}$$

$$\text{Sino } c_i = a_{i-1} \cdot c_{i-1} \pmod n$$

Fin si

$$k_i = \left\lfloor \frac{k_{i-1}}{2} \right\rfloor$$

$$i = i + 1$$

Fin mientras

$$a^k \equiv a_{i-1} \cdot c_{i-1} \pmod n$$

El siguiente ejemplo ilustrará cómo se aplica este algoritmo.

Ejemplo 1.44

Calcular $72^{21} \pmod{141}$

Solución

En este caso, $a_0 = 72$, $c_0 = 1$ y $k_0 = 21$. A fin de ordenar los cálculos, se diseña la siguiente tabla:

i	a_i	c_i	k_i
0	72	1	21
1	108	72	10
2	102	72	5
3	111	12	2
4	54	12	1

Los detalles de los datos que figuran en la tabla se explican a continuación:

Para $i = 1$

$$a_1 = a_0^2 = (72)^2 = 5184 \equiv 108 \pmod{141}$$

$$c_1 = a_0 \cdot c_0 = (72) \cdot 1 = 72 \pmod{141}$$

$$k_1 = \left\lfloor \frac{k_0}{2} \right\rfloor = \left\lfloor \frac{21}{2} \right\rfloor = 10$$

Para $i = 2$

$$a_2 = a_1^2 = (108)^2 = 11664 \equiv 102 \pmod{141}$$

$$c_2 = c_1$$

$$k_2 = \left\lfloor \frac{k_1}{2} \right\rfloor = \left\lfloor \frac{10}{2} \right\rfloor = 5$$

Para $i = 3$

$$a_3 = a_2^2 = (102)^2 = 10404 \equiv 111 \pmod{141}$$

$$c_3 = a_2 \cdot c_2 = (102) \cdot (72) = 7344 \equiv 12 \pmod{141}$$

$$k_3 = \left\lfloor \frac{k_2}{2} \right\rfloor = \left\lfloor \frac{5}{2} \right\rfloor = 2$$

Para $i = 4$

$$a_4 = a_3^2 = (111)^2 = 12321 \equiv 54 \pmod{141}$$

$$c_4 = c_3$$

$$k_4 = \left\lfloor \frac{k_3}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = 1$$

Como $k_4 \leq 1$ el proceso se detiene y por lo tanto:

$$(72)^{21} \equiv a_4 \cdot c_4 = (54) \cdot (12) = 648 \equiv 84 \pmod{141}$$

Del inciso 1) de la Proposición 1.30 resulta que 84 es el resto de la división entera de 72^{21} por 141. Luego, $72^{21} = 84 \pmod{141}$.

Grupos y Subgrupos

Definición 1.45: Grupo

Sea G un conjunto no vacío y $*$ una operación binaria definida sobre los elementos de G . El par $(G, *)$ es un grupo si y sólo si verifica las siguientes propiedades:

- 1) $*$ es Ley de Composición Interna: Si $a, b \in G \Rightarrow a * b \in G$.
- 2) Propiedad asociativa: Si $a, b \in G \Rightarrow (a * b) * c = a * (b * c)$
- 3) Existencia de elemento neutro o Identidad: $\exists e \in G / a * e = e * a \quad \forall a \in G$.
- 4) Existencia de inversos: $\forall a \in G \exists a^{-1} \in G / a * a^{-1} = a^{-1} * a = e$.

Definición 1.46: Grupo Abeliano

Un grupo $(G, *)$ es abeliano si verifica la Propiedad conmutativa. Es decir,

$$\text{Si } a, b \in G \Rightarrow a * b = b * a.$$

Ejemplo 1.47

Si $n \in \mathbb{N}$ es primo entonces, por el Corolario 1.42, $(\mathbb{Z}_n - \{0\}, \cdot)$ es un Grupo.

Proposición 1.48

Sea $G = \{ x \in \mathbb{Z}_n / \text{mcd}(x, n) = 1 \}$ entonces G es un grupo finito bajo la operación multiplicación en $\mathbb{Z}_n$.

Demostración

Las propiedades 1-3 de la definición de Grupo se verifican sin dificultad. Por otro lado, como $\text{mcd}(x, n) = 1$ entonces, por el Teorema 1.41, todo elemento de G es invertible. Por lo tanto, G es un grupo finito bajo la multiplicación en $\mathbb{Z}_n$. ■

Definición 1.49: Subgrupo

Sea $(G, *)$ un grupo y $\emptyset \neq H \subset G$. Se dice que $(H, *)$ es un subgrupo de $(G, *)$ sii $(H, *)$ es grupo.

Definición 1.50: Potencia de un elemento de un grupo

Sea $(G, *)$ un grupo y “e” su elemento neutro. Si $x \in G$ y $n \in \mathbb{N}$ entonces:

$$1) x^n = \underbrace{x * x * \dots * x}_{n \text{ veces}}$$

$$2) x^{-n} = \underbrace{x^{-1} * x^{-1} * \dots * x^{-1}}_{n \text{ veces}}$$

$$3) x^0 = e$$

La siguiente Proposición prueba algunas propiedades elementales de la potencia de un elemento de un Grupo que serán utilizadas con frecuencia.

Proposición 1.51

Sea $(G, *)$ un grupo. Si $a, b \in G$ y $m, n \in \mathbb{N}$ entonces:

$$1) a^m * a^n = a^{m+n} \qquad 4) a^{-n} = (a^n)^{-1}$$

$$2) (a^m)^n = a^{m \cdot n} \qquad 5) a^m * a^{-n} = a^{m-n}$$

$$3) (a^{-m})^n = a^{-m \cdot n} \qquad 6) \text{ Si } (G, *) \text{ es abeliano entonces } (a * b)^n = a^n * b^n$$

Demostración: Véase [4], pág. 30. ■

Definición 1.52: Subgrupo generado por un elemento del grupo

Sea $(G, *)$ un grupo y $x \in G$. El “subgrupo generado por x ”, simbolizado por $\langle x \rangle$, es

$$\langle x \rangle = \{x^k / k \in \mathbb{Z}\}$$

La siguiente Proposición es útil para caracterizar al subgrupo generado por un elemento de un grupo:

Proposición 1.53

Sea $(G, *)$ un grupo finito, e su elemento neutro y $x \in G$. Entonces

1) $\langle x \rangle$ es un subgrupo de G .

2) $\exists n_0 \in \mathbb{N}$ tal que $n_0 = \min \{n \in \mathbb{N} / x^n = e\}$

3) $\langle x \rangle = \{x^1, x^2, \dots, x^{n_0} = e\}$

Demostración

Véase [11] ■

Ejemplo 1.54

En $(\mathbb{Z}_{11}, \cdot)$, se puede comprobar que $\min \{n \in \mathbb{N} / 3^n = 1\} = 5$ pues $3^5 = 1$ en $\mathbb{Z}_{11}$ y $3^i \neq 1 \forall i=1,2,3,4$. Luego, por la Proposición 1.51 se tiene que

$$\langle 3 \rangle = \{3^1, 3^2, 3^3, 3^4, 3^5\} = \{3, 9, 5, 4, 1\}.$$

Definición 1.55: Orden de un elemento de un grupo

Sea $(G, *)$ un grupo finito, e su elemento neutro y $x \in G$. El “orden de x ”, simbolizado por $\text{ord}(x)$, es

$$\text{ord}(x) = \min \{n \in \mathbb{N} / x^n = e\}$$

Proposición 1.56

Sea $G = \{x \in \mathbb{Z}_n / x \text{ es invertible}\}$ y $a \in G$. Entonces

- 1) $\langle a \rangle = \{a^k \pmod{n} / k \in \mathbb{Z}\}$ es un subgrupo de G .
- 2) $\exists r \in \mathbb{N} / r = \min \{k \in \mathbb{N} / a^k \equiv 1 \pmod{n}\}$
- 3) $\langle a \rangle = \{a^1, a^2, \dots, a^{r-1}, a^r \equiv 1\}$
- 4) $r < n$
- 5) $\text{ord}(a) = r$

Demostración

Sea $x \in G$. Como x es invertible, por el Teorema 1.41 resulta que $\text{mcd}(x, n) = 1$. En consecuencia, por el Teorema 1.47 se tiene que G es un grupo bajo la operación multiplicación en $\mathbb{Z}_n$.

Luego, los incisos 1), 2) y 3) se deducen del Teorema 1.52.

4) Como $\langle a \rangle$ es un subgrupo de G y $G \subset \mathbb{Z}_n$ entonces $\langle a \rangle \subset G \subset \mathbb{Z}_n - \{0\}$. Entonces

$$\text{card}(\langle a \rangle) \leq \text{card}(G) \leq \text{card}(\mathbb{Z}_n - \{0\})$$

Donde $\text{card}(\langle a \rangle)$, $\text{card}(G)$ y $\text{card}(\mathbb{Z}_n - \{0\})$ representan la cantidad de elementos que tienen $\langle a \rangle$, G y $\mathbb{Z}_n - \{0\}$ respectivamente. Por lo tanto

$$\text{card}(\langle a \rangle) \leq \text{card}(\mathbb{Z}_n - \{0\}) \Rightarrow r \leq n - 1 \Rightarrow r < n$$

5) Es consecuencia inmediata de la Definición 1.55 y del inciso 2). ■

Los siguientes Teoremas y Proposiciones serán también aplicados en la justificación del Algoritmo de Shor.

Teorema 1.57: Teorema Chino del Resto

Sean $n_1, n_2, \dots, n_k$ números naturales coprimos dos a dos. Entonces, dados los enteros $a_1, a_2, \dots, a_k$, existe un entero x que es solución del sistema

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \cdot \\ \cdot \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Más aún, todas las soluciones x de este sistema son congruentes módulo el producto $n = n_1 \cdot n_2 \cdot \dots \cdot n_k$.

Demostración: Véase [12] ■

Proposición 1.58

Sean $n, n_1, n_2 \in \mathbb{N}$ tales que $n = n_1 \cdot n_2$ con n impar $\wedge n_1, n_2 \neq 1$. Si x es tal que

$$\begin{cases} x \equiv 1 \pmod{n_1} \\ x \equiv -1 \pmod{n_2} \end{cases}$$

Entonces $x \not\equiv \pm 1 \pmod{n}$

Demostración

Como $x \equiv 1 \pmod{n_1}$ entonces

$$x \not\equiv -1 \pmod{n_1} \quad [1]$$

Pues si se supone por el absurdo que $x \equiv -1 \pmod{n_1}$, por transitividad resulta que $1 \equiv -1 \pmod{n_1}$. Luego,

$$n_1 | (1 - (-1)) \Rightarrow n_1 | 2 \Rightarrow n_1 = 1 \vee n_1 = 2$$

Pero esto es una contradicción pues n es impar y $n_1 \neq 1$.

De manera similar se prueba que, como $x \equiv -1 \pmod{n_2}$ entonces

$$x \not\equiv 1 \pmod{n_2} \quad [2]$$

Por otro lado, de la ecuación [1] resulta que

$$x \not\equiv -1 \pmod{n}$$

Pues si se supone nuevamente por el absurdo que

$$\begin{aligned} x \equiv -1 \pmod{n} &\Rightarrow n | (x - (-1)) \Rightarrow n | (x + 1) \Rightarrow x + 1 = k n \text{ para algún } k \in \mathbb{Z} \\ &\Rightarrow x + 1 = (k n_2) \cdot n_1 \Rightarrow n_1 | (x + 1) \Rightarrow x \equiv -1 \pmod{n_1} \end{aligned}$$

Pero esto es una contradicción por [1]. De manera similar, se prueba que

$$x \not\equiv 1 \pmod{n}$$

Por lo tanto, $x \not\equiv \pm 1 \pmod{n}$. ■

Proposición 1.59

Sea $1 < n \in \mathbb{N}$ tal que $n \neq a^k \quad \forall a \text{ primo} \wedge \forall k \in \mathbb{N}$ entonces

$$n = p \cdot q$$

Con $p \wedge q$ coprimos.

Demostración

Por el Teorema Fundamental de la Aritmética (Teorema 1.28) se tiene que

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

Donde

$p_1 < p_2 < \dots < p_m$ son números primos y $m, \alpha_i \in \mathbb{N} \quad \forall i = 1, 2, \dots, m$. En este caso, $m \geq 2$ pues si $m < 2$ entonces $m = 1$. Luego,

$$n = p_1^{\alpha_1}$$

Esto contradice la hipótesis, ya que $n \neq a^k \quad \forall a \text{ primo} \wedge \forall k \in \mathbb{N}$. Por lo tanto, tomando $p = p_1^{\alpha_1}$ y $q = p_2^{\alpha_2} \dots p_m^{\alpha_m}$ resulta

$$n = p \cdot q$$

Además, $p \wedge q$ son coprimos pues, si se supone por el absurdo que no lo son, entonces

$$\text{mcd}(p, q) = \text{mcd}(p_1^{\alpha_1}, p_2^{\alpha_2} \dots p_m^{\alpha_m}) = d, \text{ con } d \neq 1.$$

Como $d \mid p_1^{\alpha_1} \wedge d \mid p_2^{\alpha_2} \dots p_m^{\alpha_m}$ resulta

$$\begin{cases} d = p_1^{k_1} \\ p_2^{\alpha_2} \dots p_m^{\alpha_m} = k \cdot d \end{cases}$$

Para algún $k, k_1 \in \mathbb{N}$ tal que $k_1 \leq \alpha_1$. Sustituyendo la primera ecuación en la segunda se obtiene

$$p_2^{\alpha_2} \dots p_m^{\alpha_m} = k \cdot p_1^{k_1}$$

En consecuencia

$$k = \frac{p_2^{\alpha_2} \dots p_m^{\alpha_m}}{p_1^{k_1}}$$

Pero esta última igualdad es una contradicción ya que $k \in \mathbb{N}$ y $\frac{p_2^{\alpha_2} \dots p_m^{\alpha_m}}{p_1^{k_1}}$ es una fracción irreducible. Luego, $\text{mcd}(p, q) = d = 1$ y por lo tanto $p \wedge q$ son coprimos. ■

Teorema 1.60

Sean $n, n_1, n_2 \in \mathbb{N}$ tales que

$$n = n_1 \cdot n_2$$

Con n impar, $n_1 \wedge n_2$ coprimos y $n_1, n_2 \neq 1$. Sea

$$G = \{ x \in \mathbb{Z}_n / x \text{ es invertible} \}$$

Entonces $\exists a \in G$ de orden par P tal que $a^{\frac{P}{2}} \neq \pm 1 \pmod{n}$

Demostración

Si se considera el siguiente sistema de congruencias:

$$\begin{cases} x \equiv 1 \pmod{n_1} \\ x \equiv -1 \pmod{n_2} \end{cases} \quad [1]$$

Entonces, por el Teorema Chino del Resto (Teorema 1.57), existe un entero x que es solución de este sistema. De la Proposición 1.58 resulta que

$$x \not\equiv \pm 1 \pmod{n} \quad [2]$$

Por otro lado, de la ecuación [1] se tiene

$$\begin{cases} n_1 | (x - 1) \\ n_2 | (x + 1) \end{cases} \Rightarrow \begin{cases} (x - 1) = k_1 \cdot n_1 \\ (x + 1) = k_2 \cdot n_2 \end{cases} \text{ para algún } k_1, k_2 \in \mathbb{Z}.$$

En consecuencia

$$(x - 1)(x + 1) = k_1 \cdot n_1 \cdot k_2 \cdot n_2 \Rightarrow x^2 - 1 = k_1 \cdot k_2 \cdot n_1 \cdot n_2 \Rightarrow x^2 - 1 = k_1 \cdot k_2 \cdot n$$

$$\Rightarrow n | (x^2 - 1)$$

Es decir,

$$x^2 \equiv 1 \pmod{n} \quad [3]$$

Considérese ahora x_r el resto de la división entera de x por n . Por lo tanto $x_r \in \mathbb{Z}_n$ y de la Proposición 1.30 inciso 8) se tiene que

$$x_r \equiv x \pmod{n} \quad [4]$$

De [2] y [4] resulta

$$x_r \not\equiv \pm 1 \pmod{n} \quad [5]$$

Además, de [3], [4] y aplicando la Proposición 1.30 inciso 7) se obtiene

$$x_r^2 \equiv 1 \pmod{n} \quad [6]$$

De esta última ecuación se deduce que x_r es invertible (su inverso es x_r) y tiene orden

2, que es par. Tomando $a = x_r$ y $P=2$, de la ecuación [5] resulta que $a^{\frac{P}{2}} \neq \pm 1 \pmod{n}$

■

Proposición 1.61

Sean $a, n \in \mathbb{N}$ con $n \neq 1$ y tal que $n = a^k$ para algún $k \in \mathbb{N}$. Entonces $k \leq \log_2(n)$.

Demostración

Obsérvese que $a \geq 2$, pues si $a = 1$ entonces $n = 1$, lo cual contradice la hipótesis.

Como $n = a^k$ entonces

$$\log_2(n) = k \log_2(a) \quad [1]$$

Por otro lado, como $a \geq 2$ entonces

$$\log_2(a) \geq \log_2(2) \Rightarrow \log_2(a) \geq 1 \Rightarrow \frac{1}{\log_2(a)} \leq 1 \quad [2]$$

Por lo tanto, de [1] y [2] resulta

$$k = \frac{\log_2(n)}{\log_2(a)} = \log_2(n) \cdot \frac{1}{\log_2(a)} \leq \log_2(n) \cdot 1 = \log_2(n). \quad \blacksquare$$

Corolario 1.62

Sean $n, k \in \mathbb{N}$. Si $\sqrt[k]{n} \notin \mathbb{N} \quad \forall k \in \mathbb{N}$ con $k \leq \log_2(n)$ entonces $\sqrt[k]{n} \notin \mathbb{N} \quad \forall k \in \mathbb{N}$.

Demostración

Se supondrá por el absurdo que $\exists k \in \mathbb{N}$ con $k > \log_2(n)$ tal que $\sqrt[k]{n} \in \mathbb{N}$.

Por lo tanto, $\sqrt[k]{n} = a$ para algún $a \in \mathbb{N}$. Entonces $n = a^k$ para algún $a \in \mathbb{N}$.

Por la Proposición 1.59 resulta que $k \leq \log_2(n)$, lo cual es una contradicción pues $k > \log_2(n)$. ■

Capítulo 2

Los Qubits

La unidad mínima de información en Computación Cuántica es el qubit, el análogo al bit en Informática Clásica.

En el capítulo introductorio se definió el qubit desde el punto de vista físico, pero en este capítulo se lo definirá desde el enfoque matemático.

Posteriormente se desarrollará el sistema cuántico formado por dos o más qubits junto con sus propiedades fundamentales: la superposición y el entrelazamiento.

Sistemas formados por un qubit

Los sistemas computacionales cuánticos formados por un qubit procesan la información utilizando un qubit. Su definición se expone a continuación.

Definición 2.1: qubit

Un qubit es un vector $\mathbf{q} \in \mathbb{C}^2$ de módulo 1. Es decir,

$$\mathbf{q} = \begin{pmatrix} \sim \\ \end{pmatrix}$$

donde $\sim$, $\in \mathbb{C}$ y verifican que $|\sim|^2 + | \quad |^2 = 1$

El hecho de que un qubit sea de módulo 1 se debe al Primer Postulado de la Física Cuántica (véase [3]). Como un qubit se puede escribir de la forma

$$\mathbf{q} = \begin{pmatrix} \sim \\ \end{pmatrix} = \sim \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Se dice que el conjunto $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ es una base ortonormal para el sistema formado por un qubit. Por otro lado, si se establece la siguiente notación:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} ; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Entonces la Definición 2.1 se puede reformular de la siguiente manera:

Definición 2.2:

Un qubit es un vector $\mathbf{q}$ de la forma

$$\mathbf{q} = \alpha |0\rangle + \beta |1\rangle$$

Donde

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{y } \alpha, \beta \in \mathbb{C} \text{ con } |\alpha|^2 + |\beta|^2 = 1$$

En este caso, el conjunto $\{ |0\rangle, |1\rangle \}$ constituye una base para el sistema formado por un qubit.

Los vectores $|0\rangle$ y $|1\rangle$ se corresponden con el 0 y 1 del bit clásico.

Si $\mathbf{q} = |0\rangle$ se dice que el qubit está en estado 0, mientras que si $\mathbf{q} = |1\rangle$ el qubit está en estado 1.

Cuando α y β no son nulos, se dice que el qubit está en **estado de superposición**, lo cual significa que se encuentra simultáneamente en los estados clásicos 1 y 0.

Ejemplo 2.3

Indicar si los siguientes vectores complejos representan qubits:

$$\text{a) } q_1 = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ i \frac{\sqrt{2}}{2} \end{pmatrix} \quad \text{b) } q_2 = \begin{pmatrix} \frac{1}{2}i \\ 0 \end{pmatrix} \quad \text{c) } q_3 = \begin{pmatrix} \frac{1}{2} + \frac{1}{2}i \\ \frac{1}{2} - \frac{1}{2}i \end{pmatrix}$$

Solución

Teniendo en cuenta que si $z = a + ib$ es un número complejo, el cuadrado de su módulo es $|z|^2 = a^2 + b^2$. Entonces

$$\text{a) } \left| \frac{\sqrt{2}}{2} \right|^2 + \left| i \frac{\sqrt{2}}{2} \right|^2 = \left(\frac{\sqrt{2}}{2} \right)^2 + \left(\frac{\sqrt{2}}{2} \right)^2 = \frac{1}{2} + \frac{1}{2} = 1$$

Luego, q_1 representa un qubit.

$$\text{b) } \left| \frac{1}{2}i \right|^2 + |0|^2 = \left(\frac{1}{2} \right)^2 + (0)^2 = \frac{1}{4} \neq 1$$

En consecuencia, q_2 no representa un qubit.

$$\text{c) } \left| \frac{1}{2} + \frac{1}{2}i \right|^2 + \left| \frac{1}{2} - \frac{1}{2}i \right|^2 = \left(\frac{1}{2} \right)^2 + \left(\frac{1}{2} \right)^2 + \left(\frac{1}{2} \right)^2 + \left(-\frac{1}{2} \right)^2 = \frac{4}{4} = 1$$

Por lo tanto, q_3 representa un qubit.

¿Cómo medir el estado de un qubit ?

Según el Principio de Superposición de la Mecánica Cuántica, mientras una partícula subatómica no interactúa con su entorno, ésta puede estar en varios estados al mismo tiempo. Es decir, se comporta como si pudiera hacer varias cosas simultáneamente. En particular, un qubit $q = \alpha |0\rangle + \beta |1\rangle$ puede estar en ambos estados: 0 y 1.

Pero curiosamente, en el instante en que es sometido a una medición, el qubit “colapsa” a uno de estos dos estados: 0 o bien 1. Esto significa que el estado de superposición desaparece y ello se debe a que, en el momento en que el electrón es observado, sólo adopta una de las dos posiciones de giro: spin arriba (estado 0) o spin abajo (estado 1).

Pero, ¿cómo saber a cuál de estos dos estados colapsará el qubit inmediatamente antes de efectuar la medición? Sólo se puede saber en términos de probabilidades y, para calcularlas, se aplica la siguiente definición, basada en el Tercer Postulado de la Mecánica Cuántica:

Definición 2.4: Medida de un qubit

Dado un sistema formado por un qubit, cuyo estado se describe mediante el vector

$$q = \alpha |0\rangle + \beta |1\rangle$$

Si al qubit se lo somete a una observación entonces:

El número $|\alpha|^2$ indica la probabilidad de encontrar el qubit del sistema en estado 0 .

Mientras que $|\beta|^2$ da la probabilidad de encontrar el qubit del sistema en estado 1 .

Ejemplo 2.5

Dado el qubit $q = \frac{1}{4}i |0\rangle + \frac{\sqrt{15}}{4} |1\rangle$

a) ¿Cuál es la probabilidad de que, al ser sometido a una medición, éste se encuentre en estado 0 o spin arriba?

b) ¿Cuál es la probabilidad de que, al ser sometido a una medición, éste se encuentre en estado 1 o spin abajo?

c) ¿Es posible que al ser observado el qubit, se encuentre simultáneamente en estado 0 y en estado 1?

Solución

a) La probabilidad de que el qubit se encuentre en estado 0 es $\left| \frac{1}{4}i \right|^2 = \frac{1}{16}$.

b) La probabilidad de que el qubit se encuentre en estado 1 es $\left| \frac{\sqrt{15}}{4} \right|^2 = \left(\frac{\sqrt{15}}{4} \right)^2 = \frac{15}{16}$.

c) No es posible que el qubit, al ser observado, se encuentre simultáneamente en los estados 0 y 1, ya que colapsará solamente a uno de estos dos estados.

Cabe preguntarse qué pasaría si las computadoras cuánticas utilizaran, para procesar los datos, más de un qubit. En estos casos los qubits comienzan a interactuar entre sí para generar un nuevo sistema físico. En la próxima sección se mostrará cómo describir su estado. Se verá que el producto tensorial desempeñará un rol importante, ya que permitirá modelar matemáticamente este tipo de sistemas.

Sistemas formados por dos qubits

Según el Cuarto Postulado de la Mecánica Cuántica (véase [3], pág.36), el estado de un sistema formado por dos qubits q_1 y q_2 queda determinado por el producto tensorial $q_1 \otimes q_2$.

A fin de simplificar la expresión de los productos tensoriales, se introducirá la siguiente notación:

Notación 2.6:

Si $x, y \in \{0, 1\}$ entonces se escribe

$$|x\rangle \otimes |y\rangle = |x\ y\rangle \text{ o bien } |x\rangle \otimes |y\rangle = |x, y\rangle \text{ o bien } |x\rangle \otimes |y\rangle = |x\rangle |y\rangle$$

Por lo tanto, si

$$q_1 = \alpha_1 |0\rangle + \beta_1 |1\rangle \quad y \quad q_2 = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

Entonces, al aplicar las propiedades del producto tensorial resulta

$$\begin{aligned} q_1 \otimes q_2 &= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) = \\ &= \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle \end{aligned}$$

Al calcular estos productos tensoriales se obtiene

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

En consecuencia,

$$q_1 \otimes q_2 = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1 & \beta_2 \\ \beta_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}$$

Como se puede comprobar, el producto tensorial de dos qubits genera un vector de 2^2 componentes. Por otro lado, según el Primer Postulado de la Mecánica Cuántica (véase [3], pág. 24), el vector de estado del sistema debe ser de módulo 1. Esto da lugar a definir un 2-qubit de la siguiente manera:

Definición 2.7: 2-qubit

Un 2- qubit es un vector $\mathbf{q} \in \mathbb{C}^4$ de módulo 1. Es decir,

$$\mathbf{q} = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

Donde $a_0, a_1, a_2, a_3 \in \mathbb{C}$ y verifican que $\sum_{i=0}^3 |a_i|^2 = 1$

Teniendo en cuenta que $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ es una base para el espacio de los 2- qubits, la Definición 2.7 se puede reformular de la siguiente manera:

Definición 2.8:

Un 2- qubit es un vector $\mathbf{q}$ de la forma

$$\mathbf{q} = a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle$$

Donde

$$a_0, a_1, a_2, a_3 \in \mathbb{C} \text{ y } \sum_{i=0}^3 |a_i|^2 = 1$$

En este caso, el conjunto $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ constituye una base para el espacio de los 2- qubits

De este modo, un 2-qubit es un vector que describe el estado de un sistema formado por dos qubits. Nuevamente, del Tercer Postulado de la Mecánica Cuántica se deduce la siguiente definición:

Definición 2.9: Medida de un 2- qubit

Dado un sistema formado por dos qubits, cuyo estado se describe mediante el 2-qubit

$$q = a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle$$

Si ambos qubits son observados entonces

$|a_0|^2$ indica la probabilidad de encontrar el primer y segundo qubit del sistema en estado 0.

$|a_1|^2$ indica la probabilidad de encontrar el primer qubit del sistema en estado 0 y el segundo qubit del sistema en estado 1.

$|a_2|^2$ indica la probabilidad de encontrar el primer qubit del sistema en estado 1 y el segundo qubit del sistema en estado 0.

$|a_3|^2$ indica la probabilidad de encontrar el primer y segundo qubit del sistema en estado 1.

Ejemplo 2.10

Se tiene un sistema cuántico formado por dos qubits, cuyo estado está definido mediante el 2-qubit $q = \frac{1}{\sqrt{3}} |00\rangle + \frac{1}{2} |10\rangle + \sqrt{\frac{5}{12}} |01\rangle$. Se ha decidido observar los dos qubits que componen el sistema.

- ¿Cuál es la probabilidad de que ambos qubits estén en estado 0?
- ¿Cuál es la probabilidad de que el primer qubit esté en estado 1 y el segundo en estado 0?
- ¿Cuál es la probabilidad de que ambos qubits estén en estado 1?

Solución

a) La probabilidad de que ambos qubits estén en estado 0 es $\left| \frac{1}{\sqrt{3}} \right|^2 = \left(\frac{1}{\sqrt{3}} \right)^2 = \frac{1}{3}$.

b) La probabilidad de que el primer qubit esté en estado 1 y el segundo en estado 0 es $\left| \frac{1}{2} \right|^2 = \left(\frac{1}{2} \right)^2 = \frac{1}{4}$.

c) La probabilidad de que ambos qubits estén en estado 1 es 0.

Como se mencionó anteriormente, al medir el estado de un qubit del sistema, únicamente es posible obtener dos resultados: estado 0 o bien estado 1. Además, antes de efectuar la medición, sólo se puede predecir en términos de probabilidades en qué estado se hallará dicho qubit. Así, el cálculo de probabilidades estará siempre presente a lo largo de este trabajo y por esta razón se introducirá la siguiente:

Notación 2.11:

$P(q_i = |0\rangle) = \text{Prob}(q_i = 0) = \text{Probabilidad de encontrar el } i\text{-ésimo qubit del sistema en estado 0.}$

$P(q_i = |1\rangle) = \text{Prob}(q_i = 1) = \text{Probabilidad de encontrar el } i\text{-ésimo qubit del sistema en estado 1.}$

Ejemplo 2.12

Se tiene un sistema cuántico formado por dos qubits, cuyo estado se describe mediante el 2-qubit

$$q = \frac{1}{2} |00\rangle + \frac{1}{4}i |01\rangle + \left(\frac{1}{2} + \frac{1}{2}i\right) |10\rangle + \frac{\sqrt{3}}{4} |11\rangle.$$

Se ha decidido efectuar la medición de ambos qubits.

- ¿Cuál es la probabilidad de que el primer qubit esté en estado 1 y el segundo en estado 0?
- ¿Cuál es la probabilidad de que el segundo qubit esté en estado 1?

Solución

$$a) P(q_1 = |1\rangle \wedge q_2 = |0\rangle) = \left| \frac{1}{2} + \frac{1}{2}i \right|^2 = \left(\frac{1}{2} \right)^2 + \left(\frac{1}{2} \right)^2 = \frac{1}{2}.$$

b) Al aplicar las propiedades del cálculo de probabilidades resulta

$$\begin{aligned} P(q_2 = |1\rangle) &= P(q_2 = |1\rangle \wedge (q_1 = |0\rangle \vee q_1 = |1\rangle)) = \\ P((q_2 = |1\rangle \wedge q_1 = |0\rangle) \vee (q_2 = |1\rangle \wedge q_1 = |1\rangle)) &= \\ = P(q_2 = |1\rangle \wedge q_1 = |0\rangle) + P(q_2 = |1\rangle \wedge q_1 = |1\rangle) &= \\ = \left| \frac{1}{4}i \right|^2 + \left| \frac{\sqrt{3}}{4} \right|^2 = \left(\frac{1}{4} \right)^2 + \left(\frac{\sqrt{3}}{4} \right)^2 = \frac{1}{16} + \frac{3}{16} = \frac{1}{4}. \end{aligned}$$

A continuación se describirán los sistemas cuánticos formados por 3 qubits, para luego generalizar a n qubits.

Sistemas formados por tres qubits

El estado de un sistema formado por tres qubits q_1 , q_2 y q_3 queda determinado, según el Cuarto Postulado de la Física Cuántica, por el producto tensorial $q_1 \otimes q_2 \otimes q_3$.

Nuevamente, a fin de simplificar la expresión de los productos tensoriales, se introduce la siguiente:

Notación 2.13:

Si $x, y, z \in \{0, 1\}$ entonces se escribe

$$\begin{aligned} |x\rangle \otimes |y\rangle \otimes |z\rangle &= |x \ y \ z\rangle \text{ o bien } |x\rangle \otimes |y\rangle \otimes |z\rangle = |x \ y\rangle |z\rangle \\ &\text{o bien } |x\rangle \otimes |y\rangle \otimes |z\rangle = |x\rangle |y\rangle |z\rangle \end{aligned}$$

Por lo tanto, si

$$q_1 = \alpha_1 |0\rangle + \beta_1 |1\rangle, \quad q_2 = \alpha_2 |0\rangle + \beta_2 |1\rangle \quad \text{y} \quad q_3 = \alpha_3 |0\rangle + \beta_3 |1\rangle$$

Entonces, al aplicar las propiedades del producto tensorial se obtiene

$$\begin{aligned} q_1 \otimes q_2 \otimes q_3 &= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \otimes (\alpha_3 |0\rangle + \beta_3 |1\rangle) \\ &= \alpha_1 \alpha_2 \alpha_3 |000\rangle + \alpha_1 \alpha_2 \beta_3 |001\rangle + \alpha_1 \beta_2 \alpha_3 |010\rangle + \alpha_1 \beta_2 \beta_3 |011\rangle + \\ &+ \beta_1 \alpha_2 \alpha_3 |100\rangle + \beta_1 \alpha_2 \beta_3 |101\rangle + \beta_1 \beta_2 \alpha_3 |110\rangle + \beta_1 \beta_2 \beta_3 |111\rangle \end{aligned}$$

Al calcular estos productos tensoriales resulta

$$\begin{aligned} |000\rangle &= |0\rangle \otimes |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \\ &= \begin{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \end{aligned}$$

Y así para los demás casos. Luego,

$$q_1 \otimes q_2 \otimes q_3 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1 & \alpha_2 & \beta_3 \\ \alpha_1 & \beta_2 & \alpha_3 \\ \alpha_1 & \beta_2 & \beta_3 \\ \beta_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \alpha_2 & \beta_3 \\ \beta_1 & \beta_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{pmatrix}$$

De este modo, el producto tensorial de 3 qubits genera un vector de 2^3 componentes. Además, por el Primer Postulado de la Física Cuántica, el vector de estado del sistema debe tener módulo 1. Esto da lugar a definir un 3-qubit de la siguiente manera:

Definición 2.14: 3-qubit

Un 3- qubit es un vector $\mathbf{q} \in \mathbb{C}^8$ de módulo 1. Es decir,

$$\mathbf{q} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)^T$$

Donde $a_i \in \mathbb{C} \quad \forall i = 0, \dots, 7$ y verifican que $\sum_{i=0}^7 |a_i|^2 = 1$

Teniendo en cuenta que

$$\{ |000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle \}$$

Es una base para el espacio de los 3- qubits, la Definición 2.14 se reescribe de la siguiente manera:

Definición 2.15:

Un 3- qubit es un vector $\mathbf{q}$ de la forma

$$\mathbf{q} = a_0 |000\rangle + a_1 |001\rangle + a_2 |010\rangle + a_3 |011\rangle + a_4 |100\rangle + a_5 |101\rangle + a_6 |110\rangle + a_7 |111\rangle$$

Donde

$$a_i \in \mathbb{C} \quad \forall i = 0, \dots, 7 \quad \text{y} \quad \sum_{i=0}^7 |a_i|^2 = 1$$

En este caso, el conjunto

$$\{ |000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle \}$$

Constituye una base para el espacio de los 3- qubits

De este modo, un 3-qubit es un vector que describe el estado de un sistema formado por tres qubits. La medida de un 3-qubit se define de manera similar a las Definiciones 2.4 y 2.9.

A continuación se definirán los n - qubits, los cuales permitirán describir el estado de un sistema formado por n qubits.

Sistemas formados por n qubits

El estado de un sistema formado por n qubits se describe mediante un n -qubit. Su definición surge del Primer y Cuarto Postulado de la Mecánica Cuántica y es la siguiente:

Definición 2.16: n -qubit

Dado un número natural n , un n - qubit es un vector $q \in \mathbb{C}^{2^n}$ de módulo 1. Es decir,

$$q = \left(a_0, a_1, \dots, a_{2^n-1} \right)^T$$

Donde $a_i \in \mathbb{C} \quad \forall i = 0, \dots, 2^n - 1$ y tales que $\sum_{i=0}^{2^n-1} |a_i|^2 = 1$

En este caso, una base del espacio de los n - qubits es

$$\left\{ |x_{n-1} x_{n-2} \dots x_1 x_0\rangle \text{ con } x_i = 0 \text{ ó } 1, i = 0, 1, \dots, n-1 \right\}$$

Donde

$$|x_{n-1} x_{n-2} \dots x_1 x_0\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \dots \otimes |x_1\rangle \otimes |x_0\rangle$$

Si se quisiera representar un n -qubit como combinación lineal de los elementos de esta base (de una manera similar a la planteada en las Definiciones 2.8 y 2.15) entonces su expresión, con esta notación, se tornaría engorrosa si n fuera muy grande.

Por esta razón se adoptará la siguiente convención, muy utilizada en Computación Cuántica:

Notación 2.17:

Si $x_i = 0$ ó 1 con $i = 0, 1, \dots, n-1$ entonces

$$|x_{n-1} x_{n-2} \dots x_1 x_0\rangle \equiv |x\rangle$$

Donde x es la representación en base 10 del número binario $x_{n-1} x_{n-2} \dots x_1 x_0$. Es decir,

$$x = 2^0 x_0 + 2^1 x_1 + \dots + 2^{n-2} x_{n-2} + 2^{n-1} x_{n-1}$$

El siguiente ejemplo ilustrará cómo aplicar esta notación.

Ejemplo 2.18

Dado el 2-qubit $q = a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle$, expresarlo según la Notación 2.17

Solución

El siguiente cuadro ilustra cómo representar cada elemento de la base del espacio de los 2-qubits:

Número binario	Representación en base 10
0 0	$0 (2^0) + 0 (2^1) = 0$
0 1	$1 (2^0) + 0 (2^1) = 1$
1 0	$0 (2^0) + 1 (2^1) = 2$
1 1	$1 (2^0) + 1 (2^1) = 3$

Por lo tanto

$$|00\rangle \equiv |0\rangle$$

$$|01\rangle \equiv |1\rangle$$

$$|10\rangle \equiv |2\rangle$$

$$|11\rangle \equiv |3\rangle$$

En consecuencia, el 2-qubit q se escribe

$$q = \sum_{i=0}^3 a_i |i\rangle.$$

Con esta nueva notación para los elementos de la base del espacio de los n -qubits, se puede extender las Definiciones 2.8 y 2.15 del siguiente modo:

Definición 2.19:

Un n -qubit es un vector $\mathbf{q}$ de la forma

$$\mathbf{q} = \sum_{i=0}^{2^n-1} a_i |i\rangle$$

Donde

$$a_i \in \mathbb{C} \quad \forall i = 0, \dots, 2^n - 1 \quad \text{y} \quad \sum_{i=0}^{2^n-1} |a_i|^2 = 1. \text{ En este caso, el conjunto}$$

$$\left\{ |0\rangle, |1\rangle, |2\rangle, \dots, |2^n-1\rangle \right\}$$

Constituye una base para el espacio de los n -qubits

La siguiente Proposición prueba que, si x es la representación en base 10 del número binario $x_{n-1} x_{n-2} \dots x_1 x_0$, el n -qubit $|x\rangle$ se corresponde con un vector en $\mathbb{C}^{2^n}$ que tiene un 1 en la posición “ x ” y 0 en el resto.

Proposición 2.20

Sea $n \in \mathbb{N}$ y $x \in \{0, 1, \dots, 2^n - 1\}$ la expresión en base 10 del número binario $x_{n-1} x_{n-2} \dots x_1 x_0$. Es decir,

$$x = 2^0 x_0 + 2^1 x_1 + \dots + 2^{n-2} x_{n-2} + 2^{n-1} x_{n-1}$$

Con $x_i = 0$ ó $1 \quad \forall i = 0, 1, \dots, n-1$.

Entonces $|x\rangle = |x_{n-1} x_{n-2} \dots x_1 x_0\rangle$ se corresponde con un vector en $\mathbb{C}^{2^n}$ que tiene un 1 en la posición “ x ” y 0 en el resto.

Demostración

Se aplicará el Principio de Inducción sobre n .

Para $n=1$

En este caso, $x \in \{0, 2^1 - 1\} = \{0, 1\}$. Luego, se presentan dos casos:

1) Si $x = 0$ entonces $|x\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, que es un vector en $\mathbb{C}^{2^1} = \mathbb{C}^2$ que tiene un 1 en la posición $x = 0$ y 0 en el resto.

2) Si $x = 1$ entonces $|x\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, que es un vector en $\mathbb{C}^{2^1} = \mathbb{C}^2$ que tiene un 1 en la posición $x = 1$ y 0 en el resto.

Se supone ahora que la propiedad es válida para n (Hipótesis Inductiva).

Es decir, si $x \in \{0, 1, 2, \dots, 2^n - 1\}$ es la expresión en base 10 del número binario $x_{n-1} x_{n-2} \dots x_1 x_0$, entonces $|x\rangle = |x_{n-1} x_{n-2} \dots x_1 x_0\rangle$ se corresponde con un vector en $\mathbb{C}^{2^n}$ que tiene un 1 en la posición x y 0 en el resto.

Se probará que la afirmación es válida para $n+1$

Sea $x \in \{0, 1, 2, \dots, 2^{n+1} - 1\}$ la expresión en base 10 del número binario $x_n x_{n-1} x_{n-2} \dots x_1 x_0$. Es decir,

$$x = \sum_{i=0}^n x_i 2^i = x_n 2^n + \sum_{i=0}^{n-1} x_i 2^i = x_n 2^n + \bar{x}$$

Donde

$$\overline{x} = \sum_{i=0}^{n-1} x_i 2^i. \quad [1]$$

De este modo,

$$x = x_n 2^n + \bar{x} \quad [2]$$

Así, de [1], $\bar{x}$ es la representación en base 10 del número binario $x_{n-1} x_{n-2} \dots x_1 x_0$.

Por lo tanto, por Hipótesis Inductiva, $|\overline{x}\rangle = |x_{n-1} \ x_{n-2} \ \dots \ x_1 \ x_0\rangle$ se corresponde con un vector en $\mathbb{C}^{2^n}$ que tiene un 1 en la posición $\overline{x}$ y 0 en el resto. Es decir,

$$\left| \overline{x} \right\rangle \approx \left\{ \begin{array}{c} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{array} \right\} \leftarrow \text{Posición } \overline{x} \right\} 2^n \text{ componentes} \quad [3]$$

Se consideran dos casos:

1) Si $x_n = 0$

Por [2] se tiene que $x = \bar{x}$. Aplicando la definición de producto tensorial, la Hipótesis Inductiva y [3] resulta

$$\begin{aligned}
|x\rangle &= |x_n \ x_{n-1} \ x_{n-2} \ \dots \ x_1 \ x_0\rangle = |x_n\rangle \otimes |x_{n-1} \ x_{n-2} \ \dots \ x_1 \ x_0\rangle = |0\rangle \otimes |\bar{x}\rangle = \\
&= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ \cdot \\ 1 \leftarrow \text{lugar } \bar{x} \\ \cdot \\ 0 \end{pmatrix} = \begin{pmatrix} 1. \begin{pmatrix} 0 \\ \cdot \\ 1 \\ 0 \end{pmatrix} \\ 0. \begin{pmatrix} 0 \\ \cdot \\ 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ \cdot \\ 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ \cdot \\ 1 \\ 0 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 0 \\ \cdot \\ 1 \leftarrow \text{lugar } \bar{x} \\ 0 \\ 0 \\ \cdot \\ 0 \\ \cdot \\ 0 \end{pmatrix} \left\{ 2^n + 2^n = 2^{n+1} \text{ componentes} \right.
\end{aligned}$$

En consecuencia, $|x\rangle$ se corresponde con un vector de $\mathbb{C}^{2^{n+1}}$ que tiene un 1 en el lugar $x = \bar{x}$ y 0 en el resto.

2) Si $x_n = 1$

En este caso, por [2] se tiene que $x = 2^n + \bar{x}$. Nuevamente, aplicando la definición de producto tensorial, la Hipótesis Inductiva y [3] resulta

$$\begin{aligned}
 |x\rangle &= |x_n \ x_{n-1} \ x_{n-2} \ \dots \ x_1 \ x_0\rangle = |x_n\rangle \otimes |x_{n-1} \ x_{n-2} \ \dots \ x_1 \ x_0\rangle = |1\rangle \otimes |\bar{x}\rangle = \\
 &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \leftarrow \text{lugar } \bar{x} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ \cdot \\ 0 \end{pmatrix} \\ 0. \begin{pmatrix} 1 \\ \cdot \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ \cdot \\ 0 \end{pmatrix} \\ 1. \begin{pmatrix} 1 \\ \cdot \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ \cdot \\ 0 \end{pmatrix} \\ 1 \leftarrow \text{lugar } 2^n + \bar{x} \end{pmatrix} \approx \begin{pmatrix} \begin{pmatrix} 0 \\ \cdot \\ 0 \end{pmatrix} \\ 1 \leftarrow \text{lugar } 2^n + \bar{x} \end{pmatrix} \left. \vphantom{\begin{pmatrix} 0 \\ \cdot \\ 0 \end{pmatrix}} \right\} 2^n + 2^n = 2^{n+1} \text{ componentes}
 \end{aligned}$$

Por lo tanto, $|x\rangle$ se corresponde con un vector de $\mathbb{C}^{2^{n+1}}$ que tiene un 1 en el lugar $x = 2^n + \bar{x}$ y 0 en el resto. ■

Se finaliza esta sección con un ejemplo donde se utiliza la representación decimal de un 5-qubit.

Ejemplo 2.21

Se tiene un sistema cuántico formado por 5 qubits, cuyo estado se describe mediante el 5-qubit

$$q = \left(\frac{1}{2} + \frac{1}{4}i \right) |1\rangle + \frac{1}{8} |5\rangle + \frac{1}{2}i |21\rangle + \frac{\sqrt{3}}{4} |25\rangle - \frac{1}{4} |30\rangle + \frac{\sqrt{11}}{8}i |31\rangle$$

- Expresar el qubit q en notación binaria.
- ¿Cuál es la probabilidad de que, al observar todos los qubits, el quinto qubit esté en estado 1 y los restantes en estado 0?
- ¿Cuál es la probabilidad de que, al medir todos los qubits, el quinto qubit esté en estado 1?

Solución

- Primeramente se expresan $|1\rangle$, $|5\rangle$, $|21\rangle$, $|25\rangle$, $|30\rangle$ y $|31\rangle$ en notación binaria:

Número decimal	Representación binaria
1	00001
5	00101
21	10101
25	11001
30	11110
31	11111

Por lo tanto

$$q = \left(\frac{1}{2} + \frac{1}{4}i \right) |00001\rangle + \frac{1}{8} |00101\rangle + \frac{1}{2}i |10101\rangle + \frac{\sqrt{3}}{4} |11001\rangle - \frac{1}{4} |11110\rangle + \frac{\sqrt{11}}{8}i |11111\rangle$$

b)

$$P(q_1 = |0\rangle \wedge q_2 = |0\rangle \wedge q_3 = |0\rangle \wedge q_4 = |0\rangle \wedge q_5 = |1\rangle) = \left| \frac{1}{2} + \frac{1}{4}i \right|^2 = \left(\frac{1}{2} \right)^2 + \left(\frac{1}{4} \right)^2 = \frac{5}{16}$$

$$c) P(q_5 = |1\rangle) = \left| \frac{1}{2} + \frac{1}{4}i \right|^2 + \left| \frac{1}{8} \right|^2 + \left| \frac{1}{2}i \right|^2 + \left| \frac{\sqrt{3}}{4} \right|^2 + \left| \frac{\sqrt{11}}{8}i \right|^2 =$$

$$= \frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \frac{1}{4} + \frac{3}{16} + \frac{11}{64} = \frac{15}{16}.$$

En la siguiente sección se expone una propiedad fascinante que gozan las partículas subatómicas y que, hasta el día de hoy, no deja de sorprender a la ciencia: el entrelazamiento cuántico.

El entrelazamiento cuántico

Las partículas subatómicas cuentan con una propiedad llamada **entrelazamiento o enredo cuántico (entanglement)** en inglés).

Este fenómeno funciona del siguiente modo:

Cuando dos o más partículas subatómicas interactúan, éstas pueden acabar entrelazadas. Esto significa que su posición u otras propiedades quedan estrechamente vinculadas mediante un proceso desconocido, hasta el día de hoy, por la ciencia moderna.

Gracias a esta particularidad, lo que le ocurre a una partícula puede afectar a la otra, aunque disten entre sí millones de años luz y no haya nada de por medio entre ellas.

Según Einstein, “**Éste es un fenómeno espeluznante a distancia...**”

Como el estado de las partículas cuánticas se describe mediante los qubits, el entrelazamiento cuántico hace que cualquier cambio en el estado de un qubit, provoque un cambio instantáneo en el otro qubit entrelazado.

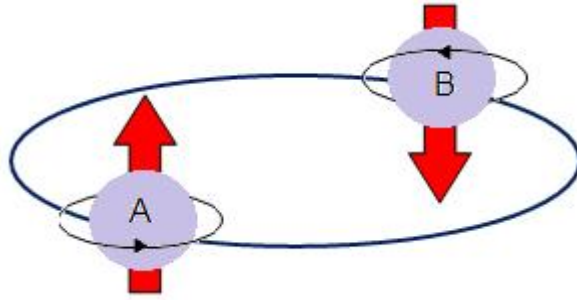


Figura 2.1: El entrelazamiento cuántico.

Este fenómeno produce que, si los electrones A y B están entrelazados, al observar o medir el estado de giro del electrón A, el electrón B recibirá automáticamente la “señal” y se mostrará girando, por ejemplo, en sentido contrario.

Pero ¿cómo se describe matemáticamente este fenómeno? Para responder a esta pregunta, se dará primeramente su correspondiente definición.

Definición 2.22: Qubits entrelazados

Dado un sistema cuántico formado por n qubits $q_1, q_2, \dots, q_n$, se dice que éstos están entrelazados si el n -qubit q , que describe el estado del sistema, no puede ser expresado como producto tensorial de los qubits que componen dicho sistema.

Más específicamente, $q_1, q_2, \dots, q_n$ están entrelazados si

$$q \div q_1 \checkmark q_2 \checkmark \dots \checkmark q_n$$

Por el contrario, si

$$q = q_1 \checkmark q_2 \checkmark \dots \checkmark q_n$$

Se dirá que los qubits $q_1, q_2, \dots, q_n$ no están entrelazados.

Ejemplo 2.23

Probar que del 2-qubit $q = \frac{1}{2} |01\rangle + \frac{\sqrt{3}}{2} |10\rangle$ se deduce que los dos qubits q_1 y q_2 que componen el sistema están entrelazados.

Solución

Se supone por el absurdo que q_1 y q_2 no están entrelazados, es decir,

$$q = q_1 \otimes q_2$$

Donde

$$\begin{aligned} q_1 &= \alpha_1 |0\rangle + \beta_1 |1\rangle \\ q_2 &= \alpha_2 |0\rangle + \beta_2 |1\rangle \end{aligned}$$

Por lo tanto, si $q = q_1 \otimes q_2$ entonces

$$\frac{1}{2} |01\rangle + \frac{\sqrt{3}}{2} |10\rangle = \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle$$

De aquí resulta el sistema de ecuaciones

$$\begin{cases} \alpha_1 \alpha_2 = 0 \\ \alpha_1 \beta_2 = \frac{1}{2} \\ \beta_1 \alpha_2 = \frac{\sqrt{3}}{2} \\ \beta_1 \beta_2 = 0 \end{cases}$$

De la primera ecuación se tiene que $\alpha_1 = 0$ ó $\alpha_2 = 0$.

Si $\alpha_1 = 0$, al reemplazar en la segunda ecuación se obtiene $0 = \frac{1}{2}$.

Similarmemente, si $\alpha_2 = 0$, al reemplazar en la tercera ecuación resulta $0 = \frac{\sqrt{3}}{2}$.

En ambos casos se llega a un absurdo, que proviene de suponer que los qubits no están entrelazados.

Ejemplo 2.24

Se tiene un sistema formado por dos qubits q_1 y q_2 , cuyo estado se expresa a través del 2-qubit $q = \frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle$. Hallar las expresiones de q_1 y q_2 para que no queden entrelazados.

Solución

Sean

$$\begin{aligned} q_1 &= \alpha_1 |0\rangle + \beta_1 |1\rangle \\ q_2 &= \alpha_2 |0\rangle + \beta_2 |1\rangle \end{aligned}$$

Se tratará de hallar las expresiones de $\alpha_1, \beta_1, \alpha_2, \beta_2$ de modo tal que q_1 y q_2 no queden entrelazados, es decir, que verifiquen la ecuación

$$q = q_1 \otimes q_2$$

Por lo tanto, si $q = q_1 \otimes q_2$ entonces

$$\frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle = \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle$$

De aquí resulta el sistema de ecuaciones

$$\left\{ \begin{array}{ll} \alpha_1 \alpha_2 = \frac{1}{2} & [1] \\ \alpha_1 \beta_2 = -\frac{1}{2} & [2] \\ \beta_1 \alpha_2 = \frac{1}{2} & [3] \\ \beta_1 \beta_2 = -\frac{1}{2} & [4] \end{array} \right.$$

Además,

$$\left\{ \begin{array}{ll} |\alpha_1|^2 + |\beta_1|^2 = 1 & [5] \\ |\alpha_2|^2 + |\beta_2|^2 = 1 & [6] \end{array} \right.$$

Se tratará de expresar β_1 , α_2 , β_2 en términos de α_1 . De las ecuaciones [1] – [3] se obtiene

$$\left\{ \begin{array}{ll} \alpha_2 = \frac{1}{2 \alpha_1} & [7] \\ \beta_2 = -\frac{1}{2 \alpha_1} & [8] \\ \beta_1 = \frac{1}{2 \alpha_2} = \frac{1}{2 \frac{1}{2 \alpha_1}} = \alpha_1 & [9] \end{array} \right.$$

Reemplazando [9] en [5] se tiene

$$|\alpha_1|^2 + |\beta_1|^2 = 1 \Rightarrow |\alpha_1|^2 + |\alpha_1|^2 = 1 \Rightarrow 2|\alpha_1|^2 = 1 \Rightarrow |\alpha_1|^2 = \frac{1}{2}$$

Luego,

$$|\alpha_1| = \frac{\sqrt{2}}{2} \quad [10]$$

De manera similar, al reemplazar [7] y [8] en [6], se obtiene la ecuación [10]. Por lo tanto, para que q_1 y q_2 no estén entrelazados, sus expresiones deben ser de la forma

$$\begin{aligned} q_1 &= \alpha_1 |0\rangle + \alpha_1 |1\rangle \\ q_2 &= \frac{1}{2\alpha_1} |0\rangle - \frac{1}{2\alpha_1} |1\rangle \end{aligned}$$

$$\text{Con } |\alpha_1| = \frac{\sqrt{2}}{2}.$$

Cabe preguntarse cómo evoluciona un sistema cuántico formado por dos o más qubits, cuando solamente algunos qubits son sometidos a observación. Las siguientes

Proposiciones responden a esta pregunta, para el caso de sistemas formados por dos o tres qubits.

Proposición 2.25

Sea un sistema compuesto por dos qubits, y cuyo estado se describe mediante el 2-qubit

$$q = a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle$$

Entonces

Si una vez realizada la medición sólo del primer qubit del sistema, se obtiene que éste está en estado 0, el 2-qubit evoluciona al siguiente estado:

$$q = \frac{a_0 |00\rangle + a_1 |01\rangle}{\sqrt{|a_0|^2 + |a_1|^2}}$$

Y si se obtiene que éste está en estado 1, el 2-qubit evoluciona a un nuevo estado dado por

$$q = \frac{a_2 |10\rangle + a_3 |11\rangle}{\sqrt{|a_2|^2 + |a_3|^2}}$$

Expresiones similares se obtienen para los resultados de la medida del segundo qubit del sistema.

Demostración

Véase [5] ■

Proposición 2.26

Sea un sistema compuesto por tres qubits, y cuyo estado se describe mediante el 3-qubit

$$q = a_0 |000\rangle + a_1 |001\rangle + a_2 |010\rangle + a_3 |011\rangle + a_4 |100\rangle + a_5 |101\rangle + a_6 |110\rangle + a_7 |111\rangle$$

Entonces

Si una vez realizada la medición de los dos primeros qubits del sistema, se obtiene que ambos están en estado 0, el 3-qubit evoluciona al siguiente estado:

$$q = \frac{a_0 |000\rangle + a_1 |001\rangle}{\sqrt{|a_0|^2 + |a_1|^2}}$$

Expresiones similares se obtienen para las restantes mediciones.

Demostración

Véase [5] ■

Las Proposición anterior se puede generalizar para el caso de sistemas formados por n qubits,

Los siguientes ejemplos muestran cómo, en caso de haber entrelazamiento, al medir el estado de un qubit se podrá predecir, con un 100% de seguridad, en qué estado estará el

otro qubit del sistema en caso de ser observado. Mientras que si los qubits no están entrelazados, la medida de un qubit no influirá en la medida del otro.

Ejemplo 2.27

Sea el sistema entrelazado presentado en el Ejemplo 2.23, determinado por el 2-qubit

$$q = \frac{1}{2} |01\rangle + \frac{\sqrt{3}}{2} |10\rangle$$

Si al medir el primer qubit del sistema se observa que éste está en estado 0, de la Proposición 2.25 resulta que el 2-qubit evoluciona al estado

$$q = |01\rangle$$

En este caso, las probabilidades de medida sobre el segundo qubit son

$$P(q_2 = |0\rangle) = 0$$

$$P(q_2 = |1\rangle) = 1$$

Esto significa que si al observar el primer qubit del sistema, éste se encuentra spin arriba (estado 0) entonces hay un 100 % de seguridad de que el segundo qubit del sistema se halle spin abajo (estado 1).

Por otro lado, si al medir el primer qubit resulta que éste se encuentra en estado 1, de la Proposición 2.25 resulta que el 2-qubit evoluciona al estado

$$q = |10\rangle$$

Y en este caso, las probabilidades de medida sobre el segundo qubit son

$$P(q_2 = |0\rangle) = 1$$

$$P(q_2 = |1\rangle) = 0$$

Lo cual significa que si al observar el primer qubit del sistema, éste se encuentra spin abajo (estado 1) entonces hay un 100 % de probabilidad de que el segundo qubit del sistema esté spin arriba (estado 0).

En ambos casos se puede comprobar que la medida del primer qubit sí afecta la medida del segundo qubit del sistema.

Ejemplo 2.28

Sea el sistema no entrelazado presentado en el Ejemplo 2.24, determinado por el 2-qubit

$$q = \frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle$$

Si al medir el primer qubit del sistema se observa que éste está en estado 0, de la Proposición 2.25 resulta que el 2-qubit evoluciona al estado

$$q = \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |01\rangle$$

En este caso, las probabilidades de medida sobre el segundo qubit son

$$P(q_2 = |0\rangle) = \left| \frac{1}{\sqrt{2}} \right|^2 = \left(\frac{1}{\sqrt{2}} \right)^2 = \frac{1}{2}$$

$$P(q_2 = |1\rangle) = \left| -\frac{1}{\sqrt{2}} \right|^2 = \left(-\frac{1}{\sqrt{2}} \right)^2 = \frac{1}{2}$$

Por otro lado, si al medir el primer qubit resulta que éste se encuentra en estado 1, nuevamente de la Proposición 2.25 resulta que el 2-qubit evoluciona al estado

$$q = \frac{1}{\sqrt{2}} |10\rangle - \frac{1}{\sqrt{2}} |11\rangle$$

Y en este caso, las probabilidades de medida sobre el segundo qubit son

$$P(q_2 = |0\rangle) = P(q_2 = |1\rangle) = \frac{1}{2}$$

En ambas situaciones se puede observar que la medida del primer qubit no influye en la medida del segundo qubit del sistema, ya que habrá un 50% de seguridad de que el segundo qubit pueda estar en estado 1 o en estado 0.

El ejemplo anterior muestra matemáticamente que, cuando dos partículas subatómicas están entrelazadas, el estado de una de ellas afecta sobre el estado de la otra, aunque se encuentren arbitrariamente alejadas entre sí y sin ningún medio físico que las una.

Capítulo 3

Compuertas y circuitos cuánticos

En Computación Clásica, para manipular la información almacenada en un conjunto de bits se utilizan compuertas lógicas. Por ejemplo, las compuertas AND, OR, NOT, XOR, NAND, etc.

En cambio, en Computación Cuántica, para manipular la información almacenada en un conjunto de qubits se utilizan compuertas cuánticas.

Desde el punto de vista de la Física, una compuerta cuántica es un dispositivo electro-magnético con n qubits de entrada y n qubits de salida, que permite modificar el estado de los qubits que ingresan. Es decir, pueden cambiar el spin de los electrones que componen el sistema.

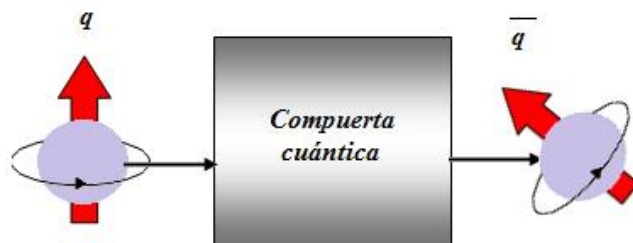


Figura 3.1: Representación gráfica de una compuerta cuántica. $\bar{q}$ es el estado en que puede quedar el qubit q al atravesar una compuerta.

Características de las compuertas cuánticas

Las compuertas cuánticas son las encargadas de realizar las operaciones, los cálculos. Tienen fundamentalmente las siguientes propiedades:

- **Reversibilidad.**
- **El número de entradas es igual al número de salidas.**

■ Reversibilidad

Una compuerta es reversible si a partir de los datos de salida se pueden recuperar los datos de entrada. Es decir, para cada compuerta debe haber otra que “deshaga” lo que hizo la primera.

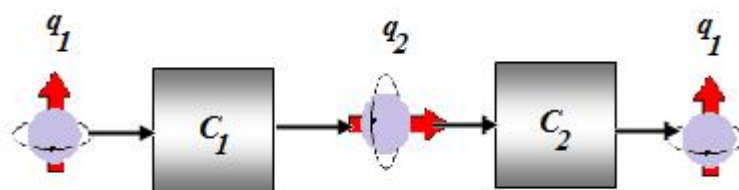


Figura 3.2: Reversibilidad de una compuerta cuántica. La compuerta C_1 modifica el estado del qubit q_1 , para transformarlo en el estado q_2 . Mientras que la compuerta C_2 revierte el estado q_2 , para recuperar el estado q_1 .

La reversibilidad de una compuerta cuántica es un requisito sumamente importante, porque los resultados de los algoritmos cuánticos se determinan en términos de probabilidades. Es por ello que un mismo algoritmo necesita ser ejecutado varias veces para poder afirmar, con cierto porcentaje de seguridad, cuáles son los resultados obtenidos. De este modo, un qubit debe ser capaz de recuperar su estado anterior a fin de “recalcular o reiterar” las operaciones indicadas en el algoritmo.

La Computación Clásica no necesita tener compuertas reversibles. La compuerta NOT es la única que sí lo es, como se ilustra en la siguiente figura.

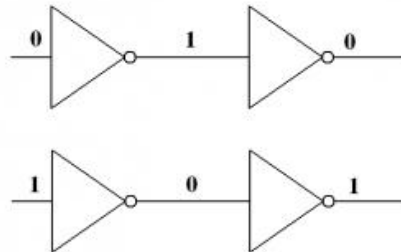


Figura 3.3: Reversibilidad de la compuerta NOT. Poniendo detrás de una compuerta NOT otra igual, se deshace lo que hizo la primera.

■ El número de entradas es igual al número de salidas

Si la compuerta cuántica tuviera menos salidas que entradas, se desecharía información. Este hecho se traduce físicamente en una disipación de la energía que se transforma en calor y, por consiguiente, estos sistemas se calentarían. Como los estados cuánticos del átomo son extremadamente frágiles, la superposición podría verse afectada ante la más mínima fluctuación de la temperatura, lo que provocaría errores de cálculo.

Por otro lado, si la compuerta tuviera más salidas que entradas, la compuerta encargada de recuperar los datos de entrada tendría menos salidas que entradas. Pero, por lo visto anteriormente, se producirían errores de cálculo.

Por esta razón una compuerta cuántica debe tener el mismo número de entradas que de salidas.

Cómo modelar matemáticamente una compuerta cuántica

Para modelar matemáticamente una compuerta cuántica, se recurre al Segundo Postulado de la Mecánica Cuántica:

Segundo Postulado de la Mecánica Cuántica:

*La evolución de un sistema cuántico **cerrado** (totalmente aislado, sin intercambio de energía con su medio ambiente) se describe mediante una transformación unitaria. Es decir que, si q_1 es el estado del sistema en el instante t_1 y q_2 es el estado en el instante t_2 , entonces existe un operador unitario U de modo tal que $q_2 = U q_1$.*

Debido a que una compuerta cuántica de n qubits es capaz de modificar o hacer evolucionar el estado de los qubits del sistema, el Segundo Postulado sugiere asociar, a cada compuerta cuántica, una transformación unitaria definida en el espacio de los n -qubits, ya que éstos describen el estado del sistema. Por otro lado, como los n -qubits se identifican con vectores en $\mathbb{C}^{2^n}$, la transformación unitaria quedará definida en

$\mathbb{C}^{2^n}$. Además, se sabe que toda transformación unitaria lleva asociada una matriz unitaria. Es por ello que de aquí surge la definición matemática de compuerta cuántica:

Definición 3.1: Compuerta cuántica

Una compuerta cuántica, de n qubits de entrada y n qubits de salida, es una matriz unitaria U de orden 2^n , es decir, una matriz $U \in \mathbb{C}^{2^n} \times \mathbb{C}^{2^n}$ que verifica

$$U U^\dagger = U^\dagger U = I$$

Donde $U^\dagger$ es la traspuesta conjugada de U e I es la matriz Identidad.

La siguiente Proposición prueba que una matriz unitaria preserva el módulo de un vector y, en consecuencia, transforma un n -qubit en otro n -qubit.

Proposición 3.2

Sea $v \in \mathbb{C}^m$ y U una matriz unitaria $m \times m$. Entonces si $\|v\| = 1 \Rightarrow \|Uv\| = 1$

Demostración

Si $v = (v_1, v_2, \dots, v_m)^T$ y $w = (w_1, w_2, \dots, w_m)^T$ entonces $\langle v, w \rangle = v^T \bar{w}$.

Por lo tanto $\|Uv\|^2 = \langle Uv, Uv \rangle = (Uv)^T \overline{Uv} = v^T U^T \overline{Uv} = v^T \overline{U^T U} v = v^T \overline{I} v = v^T I v = v^T v = \langle v, v \rangle = \|v\|^2$.

En consecuencia, $\|Uv\|^2 = \|v\|^2$.

De aquí resulta que $\|v\| = 1 \Rightarrow \|v\|^2 = 1 \Rightarrow \|Uv\|^2 = 1 \Rightarrow \|Uv\| = 1$ ■

Circuitos Cuánticos

Para cualquier cómputo cuántico se necesita diseñar un circuito cuántico, el cual se define de la siguiente manera:

Definición 3.3: Circuito cuántico

Un circuito cuántico es un dispositivo que consta de los siguientes elementos:

- 1) **Uno o más qubits de entrada.** Éstos sólo pueden estar inicializados en $|0\rangle$ o en $|1\rangle$ ya que el electrón, al interactuar con el medio ambiente, puede estar únicamente en dos estados: spin arriba o spin abajo.
- 2) **Una o más compuertas cuánticas.** Éstas permiten modificar el estado de uno o más qubits que componen el sistema.
- 3) **Uno o más qubits de salida.** Ellos son el resultado de los cálculos realizados por las compuertas cuánticas. La medición final se efectúa sobre algunos de los qubits de salida. La cantidad de qubits de salida debe ser igual a la de entrada.

En la representación gráfica de un circuito cuántico, las compuertas cuánticas se simbolizan mediante rectángulos. Cada qubit de entrada o de salida debe ir acompañado de un cable o segmento horizontal. El proceso de medición convierte el estado de un qubit $q = \alpha |0\rangle + \beta |1\rangle$ en un “bit clásico”, que será 0 con una probabilidad $|\alpha|^2$ o bien 1 con una probabilidad $|\beta|^2$.

El procedimiento de medición de un qubit se lo simboliza así:



Figura 3.4: Representación gráfica del proceso de medición de un qubit q . Las líneas dobles se utilizan para simbolizar los bits clásicos: 0 y 1.

El gráfico de un circuito se lee de izquierda a derecha. La siguiente figura muestra un circuito cuántico formado por dos qubits de entrada:

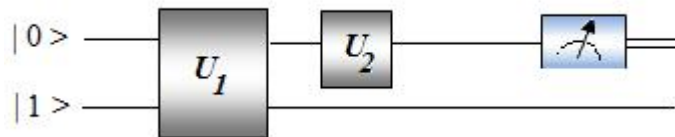


Figura 3.5: Un ejemplo de circuito cuántico.

Las compuertas cuánticas más utilizadas son las de un qubit y dos qubits. Ello se debe a que cualquier circuito cuántico puede diseñarse empleando solamente este tipo de compuertas. Por esta razón, en la siguiente sección, se las describirá detalladamente.

Compuertas cuánticas de un qubit

Desde el punto de vista físico, las compuertas cuánticas que operan sobre un qubit son dispositivos que modifican el spin del electrón. Esto se logra generando campos magnéticos a lo largo de diferentes direcciones, los cuales permiten cambiar la orientación del spin del electrón. Pero desde el punto de vista matemático, según el Corolario 3.1, las compuertas cuánticas que operan sobre un qubit se representan mediante matrices unitarias de orden 2.

Teóricamente, cualquier matriz unitaria de orden 2 define una compuerta cuántica de un qubit. Sin embargo, las más utilizadas se presentarán a continuación.

Principales compuertas cuánticas de un qubit

En esta sección se definirán las principales compuertas cuánticas de un qubit en términos de sus matrices unitarias asociadas.

Las matrices de Pauli

Las matrices de Pauli son tres: X , Y , Z donde

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Para analizar el efecto que tienen las compuertas asociadas a estas matrices sobre un qubit, basta hacerlo sobre los qubits $|0\rangle$ y $|1\rangle$, ya que éstos constituyen una base para el sistema formado por un qubit. En particular, el resultado que produce la compuerta X es:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

De este modo, esta compuerta cambia el estado 0 al estado 1 y el estado 1 al estado 0. Por esta razón a la matriz de Pauli X se la suele llamar “la compuerta NOT”. Físicamente significa que, si el electrón estaba “spin arriba”, al atravesar la compuerta X pasa a estar “spin abajo” y viceversa.



Figura 3.6: Efecto de la matriz X sobre los qubits de la base.

Si ahora se considera un qubit genérico $q = \alpha|0\rangle + \beta|1\rangle$ entonces, al aplicar la compuerta X, se obtiene $Xq = X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle$. Es decir,

$$X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$$

De este modo, invierte los coeficientes α y β del qubit q .

Por otro lado, el efecto de la matriz Z sobre los qubits de la base es:

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

Es decir que, al estado 0 lo deja inalterado y al estado 1 le cambia el signo.

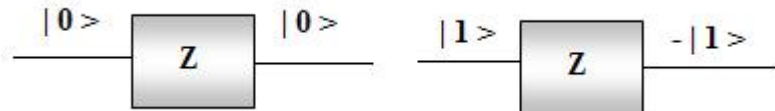


Figura 3.7: Efecto de la matriz Z sobre los qubits de la base.

Si ahora se considera un qubit genérico $q = \alpha|0\rangle + \beta|1\rangle$ entonces, al aplicar la compuerta Z, se obtiene

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

Luego, a la componente α la deja intacta, mientras que a la componente β le cambia el signo.

Obsérvese, además, que la compuerta Y se puede expresar como $Y = i X \cdot Z$

La compuerta de Hadamard

Esta compuerta es sumamente relevante y lleva este nombre en honor al matemático francés Jacques Hadamard (1865-1963). Su matriz asociada es la siguiente:

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

A continuación se muestra cómo actúa esta matriz sobre los qubits de la base:

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

$$H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$$

Como se puede comprobar, la compuerta de Hadamard transforma los qubits $|0\rangle$ y $|1\rangle$ en estados de superposición, permitiendo estar en estado 0 y 1 al mismo tiempo. Por otro lado, los qubits transformados $H|0\rangle$ y $H|1\rangle$ tienen la misma probabilidad de que colapsen a estado 0 o a estado 1 en el instante en que entren en contacto con el medio ambiente (es decir, en el momento en que sean observados o sean sometidos a

una medición). El valor de dicha probabilidad es $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$.

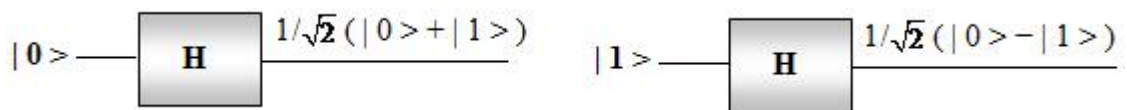


Figura 3.8: Efecto de la compuerta H sobre los qubits de la base.

Físicamente la superposición se logra creando una “trampa de iones”. Sin embargo, es muy difícil mantenerla en el tiempo, ya que el electrón debe estar completamente aislado, porque si interactúa con el medio ambiente, el estado de superposición se destruye. Esta es una de las causas principales por la cual se torna muy dificultosa la construcción de computadoras cuánticas.

La compuerta R o de desplazamiento de fase

Dado un ángulo θ expresado en radianes, la compuerta de desplazamiento de fase R_θ tiene la siguiente forma matricial:

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

El efecto de esta compuerta sobre los qubits de la base es el siguiente:

$$R_\theta |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$R_\theta |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ e^{i\theta} \end{pmatrix} = e^{i\theta} |1\rangle$$

Es decir que al qubit $|0\rangle$ lo deja intacto y a $|1\rangle$ lo transforma en $e^{i\theta} |1\rangle$.

La compuerta R_θ , junto con la de Hadamard, serán utilizadas para diseñar el circuito cuántico para la Transformada Cuántica de Fourier.

Las matrices de Pauli cobran importancia debido a que cualquier matriz unitaria de orden 2 puede escribirse, junto con la matriz Identidad, como combinación lineal de estas matrices (Véase [3]).

Ejemplo 3.4

Sea el qubit de entrada $q = |x\rangle$, con $x \in \{0, 1\}$ y el circuito:

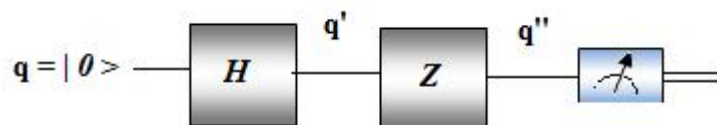


- 1) Indicar el estado del qubit al atravesar cada compuerta.
- 2) Si el qubit de entrada es $q = |0\rangle$, ¿Cuál es la probabilidad de que, al observar el qubit de salida, esté en estado 0?
- 3) ¿Podría diseñarse el circuito mediante una única compuerta cuántica?

Solución

- 1) Se simbolizará por q' y q'' a los estados del qubit q al atravesar las compuertas H y Z respectivamente.

Primer Caso: $q = |0\rangle$



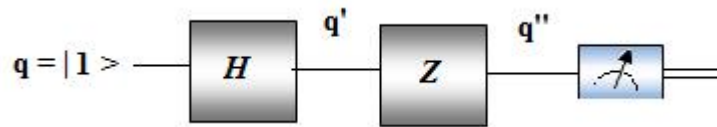
Al aplicar el Segundo Postulado de la Mecánica Cuántica, los estados del qubit se obtienen del siguiente modo:

$$q = |0\rangle$$

$$q' = H \ q = H \ |0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$q'' = Z \ q' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Segundo Caso: $q = |1\rangle$



Nuevamente, aplicando el Segundo Postulado de la Mecánica Cuántica resulta

$$q = |1\rangle$$

$$q' = H \ q = H \ |1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$q'' = Z \ q' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

2) Si $q = |0\rangle$, el qubit de salida del sistema es

$$q'' = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ . Por lo tanto,}$$

$$P(q'' = |0\rangle) = \left| \frac{1}{\sqrt{2}} \right|^2 = \left(\frac{1}{\sqrt{2}} \right)^2 = \frac{1}{2}$$

3) Debido a que el producto de matrices unitarias es una matriz unitaria, el circuito puede diseñarse mediante una única compuerta cuántica definiendo la matriz

$$U = Z \cdot H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

Ejemplo 3.5

Construir una compuerta cuántica que lleve el qubit $|0\rangle$ al qubit $-|0\rangle$.

Solución

Se deberá hallar una matriz unitaria U de orden 2 tal que $U \cdot |0\rangle = -|0\rangle$.

Por lo tanto, si

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Entonces

$$U|0\rangle = -|0\rangle \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

De aquí resulta

$$\begin{cases} a = -1 \\ c = 0 \end{cases} \quad [1]$$

Por otro lado, como U es una matriz unitaria y haciendo uso de [1], se tiene

$$\begin{aligned} U U^T &= I \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} -1 & b \\ 0 & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \\ \Rightarrow \begin{pmatrix} 1 + |b|^2 & b \bar{d} \\ d \bar{b} & |d|^2 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Luego,

$$\begin{cases} 1 + |b|^2 = 1 \\ |d|^2 = 1 \end{cases} \Rightarrow \begin{cases} |b|^2 = 0 \\ |d| = 1 \end{cases} \Rightarrow \begin{cases} b = 0 \\ |d| = 1 \end{cases} \quad [2]$$

De [1] y [2] resulta

$$U = \begin{pmatrix} -1 & 0 \\ 0 & d \end{pmatrix}$$

Con $|d| = 1$

O equivalentemente, si se expresa el número complejo “ d ” en forma exponencial entonces

$$U = \begin{pmatrix} -1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Con $0 \leq \theta < 2\pi$

Compuertas cuánticas de dos qubits

Una compuerta cuántica que opera sobre un sistema formado por dos qubits es una matriz unitaria de orden 2^2 . Como se sabe, una base ortonormal para el espacio de los 2-qubits es

$$\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$$

Donde

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \approx \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \approx \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \approx \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Luego, para definir la matriz unitaria U asociada a una compuerta cuántica, bastará con definir la transformación U sobre cada 2-qubit de la base, expresándola como combinación lineal de los elementos de dicha base. Es decir, se especificará:

$$U|00\rangle = a_{11}|00\rangle + a_{12}|01\rangle + a_{13}|10\rangle + a_{14}|11\rangle$$

$$U|01\rangle = a_{21}|00\rangle + a_{22}|01\rangle + a_{23}|10\rangle + a_{24}|11\rangle$$

$$U|10\rangle = a_{31}|00\rangle + a_{32}|01\rangle + a_{33}|10\rangle + a_{34}|11\rangle$$

$$U|11\rangle = a_{41}|00\rangle + a_{42}|01\rangle + a_{43}|10\rangle + a_{44}|11\rangle$$

De este modo, la matriz unitaria U será

$$U = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

A continuación se describirán las principales compuertas cuánticas aplicables a un sistema de dos qubits.

Principales compuertas cuánticas de dos qubits

La compuerta Swap

Esta compuerta intercambia dos qubits. Se la define por

$$\text{Swap} |x y\rangle = |y x\rangle \text{ con } x, y \in \{0, 1\}.$$

La representación gráfica es la siguiente:

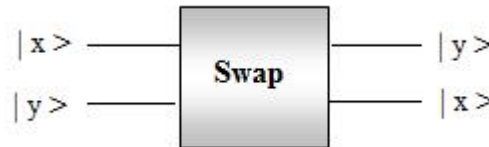


Figura 3.9: Representación gráfica de la compuerta Swap.

El efecto de esta compuerta sobre cada 2-qubit de la base es:

$$\text{Swap} |00\rangle = |00\rangle = 1 \cdot |00\rangle + 0 \cdot |01\rangle + 0 \cdot |10\rangle + 0 \cdot |11\rangle$$

$$\text{Swap} |01\rangle = |10\rangle = 0 \cdot |00\rangle + 0 \cdot |01\rangle + 1 \cdot |10\rangle + 0 \cdot |11\rangle$$

$$\text{Swap} |10\rangle = |01\rangle = 0 \cdot |00\rangle + 1 \cdot |01\rangle + 0 \cdot |10\rangle + 0 \cdot |11\rangle$$

$$\text{Swap} |11\rangle = |11\rangle = 0 \cdot |00\rangle + 0 \cdot |01\rangle + 0 \cdot |10\rangle + 1 \cdot |11\rangle$$

Por lo tanto, la matriz asociada a esta compuerta es

$$U_{\text{swap}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Observación 3.6: En general, a la matriz asociada a una compuerta cuántica se la suele nombrar anteponiendo la letra “U”.

La compuerta Xor

Antes de describir esta compuerta, y para comprender porqué lleva este nombre, se recordará que el operador lógico Xor, también llamado “O excluyente”, tiene la siguiente tabla de valores:

x	y	x Xor y
0	0	0
0	1	1
1	0	1
1	1	0

Como se puede comprobar, este operador lógico coincide con la “suma módulo 2” que, como se mencionó en el capítulo anterior, se lo representa con el símbolo $\oplus$.

La compuerta cuántica Xor se la define a través de la transformación unitaria

$$\text{Xor} |x y\rangle = |x, x \oplus y\rangle$$

Con $x, y \in \{0, 1\}$.

En este caso, el primer qubit recibe el nombre de “*qubit de control*”, pues permanece inalterado. Mientras que el segundo qubit se lo llama “*qubit objetivo*”. Obsérvese que si el qubit de control vale 0, el objetivo no cambia, mientras que si vale 1, se niega el objetivo.

La representación gráfica de esta compuerta es:

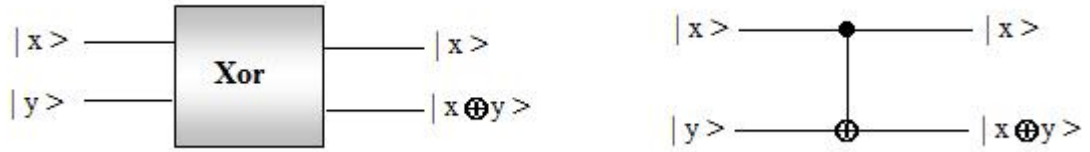


Figura 3.10: Dos representaciones gráficas de la compuerta Xor.

Por lo tanto

$$\text{Xor} |0 0\rangle = |0, 0 \oplus 0\rangle = |0 0\rangle$$

$$\text{Xor} |0 1\rangle = |0, 0 \oplus 1\rangle = |0 1\rangle$$

$$\text{Xor} |1 0\rangle = |1, 1 \oplus 0\rangle = |1 1\rangle$$

$$\text{Xor} |1 1\rangle = |1, 1 \oplus 1\rangle = |1 0\rangle$$

Su expresión matricial es entonces

$$U_{\text{Xor}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

La compuerta Xor es de gran importancia ya que cualquier compuerta de n qubits puede ser construida mediante la compuerta Xor y compuertas de un qubit. La demostración de esta afirmación supera el objetivo de este trabajo. Sin embargo, a modo ilustrativo, en el siguiente ejemplo se mostrará cómo la compuerta Swap puede ser implementada mediante tres compuertas Xor.

La compuerta Xor

Es similar a la compuerta Xor y se la define por

$$\overline{\text{Xor}} |x y\rangle = |x \oplus y, y\rangle$$

Con $x, y \in \{0, 1\}$.

En este caso el primer qubit recibe el nombre de “*qubit objetivo*” y al segundo qubit, al permanecer inalterado, se lo llama “*qubit de control*”.

Su representación gráfica es:

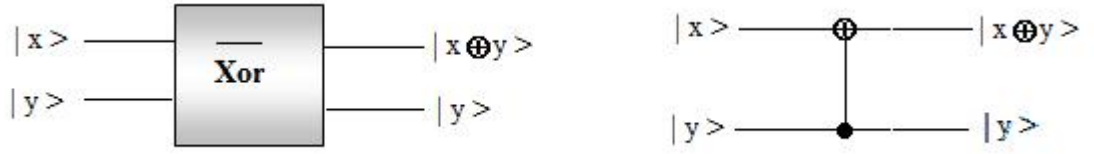


Figura 3.11: Dos representaciones gráficas de la compuerta $\overline{Xor}$.

Se prueba, de manera similar a los casos anteriores, que la matriz asociada a esta compuerta es

$$\overline{U_{xor}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

La compuerta de Hadamard para un sistema de dos qubits

Se la define por

$$H^{\otimes 2} |x y\rangle = H |x\rangle \otimes H |y\rangle$$

Con $x, y \in \{0, 1\}$

El efecto de esta compuerta sobre cada 2-qubit de la base es

$$H^{\otimes 2} |0 0\rangle = H |0\rangle \otimes H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|0 0\rangle + |0 1\rangle + |1 0\rangle + |1 1\rangle)$$

$$H^{\otimes 2} |0 1\rangle = H |0\rangle \otimes H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|0 0\rangle - |0 1\rangle + |1 0\rangle - |1 1\rangle)$$

$$H^{\otimes 2} |1 0\rangle = H |1\rangle \otimes H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|0 0\rangle + |0 1\rangle - |1 0\rangle - |1 1\rangle)$$

$$H^{\otimes 2} |1 1\rangle = H |1\rangle \otimes H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|0 0\rangle - |0 1\rangle - |1 0\rangle + |1 1\rangle)$$

Luego, su representación matricial es

$$H^{\otimes 2} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

La compuerta de Hadamard puede generalizarse para un sistema formado por n qubits, como se verá en la próxima sección.

La compuerta f

A partir de una función booleana $f: \{0, 1\} \rightarrow \{0, 1\}$ se puede construir una compuerta cuántica de dos qubits, llamada la compuerta f , mediante una transformación unitaria U_f definida del siguiente modo:

$$U_f |x\rangle |y\rangle = |x\rangle, |y \oplus f(x)\rangle$$

Donde $\oplus$ representa la suma módulo 2 y $x, y \in \{0, 1\}$.

Por lo tanto, la compuerta cuántica asociada a U_f opera del siguiente modo:

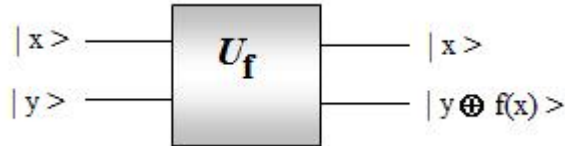


Figura 3.12: Efecto de la compuerta f .

Obsérvese que la compuerta Xor es un caso particular de la compuerta f , considerando $f(x) = x$. El siguiente ejemplo muestra cómo funciona la compuerta f .

Ejemplo 3.6

Dada $f: \{0, 1\} \rightarrow \{0, 1\}$ definida por $f(0) = 1$, $f(1) = 0$, hallar la matriz asociada a la transformación U_f .

Solución

$$U_f |00\rangle = |0, 0 \oplus f(0)\rangle = |0, 0 \oplus 1\rangle = |01\rangle$$

$$U_f |01\rangle = |0, 1 \oplus f(0)\rangle = |0, 1 \oplus 1\rangle = |00\rangle$$

$$U_f |10\rangle = |1, 0 \oplus f(1)\rangle = |1, 0 \oplus 0\rangle = |10\rangle$$

$$U_f |11\rangle = |1, 1 \oplus f(1)\rangle = |1, 0 \oplus 1\rangle = |11\rangle$$

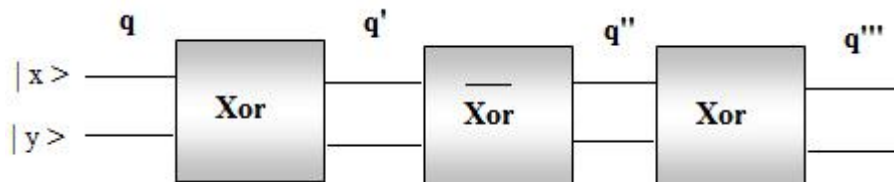
Luego, la matriz asociada es

$$U_f = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

El circuito que se muestra a continuación intercambia dos qubits mediante el uso de tres Xor cuánticos.

Ejemplo 3.7

Dados los qubits de entrada $q_1 = |x\rangle$, $q_2 = |y\rangle$, con $x, y \in \{0, 1\}$, y el siguiente circuito:



- a) Indicar el estado del sistema al atravesar cada compuerta.
b) ¿Qué efecto tiene el circuito sobre los qubits de entrada?

Solución

a) Por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema se expresa mediante el producto tensorial de q_1 con q_2 , es decir

$$q = q_1 \otimes q_2 = |x\rangle \otimes |y\rangle = |x, y\rangle$$

Por otro lado, teniendo en cuenta que $x \oplus x = 0 \quad \forall x \in \{0, 1\}$, el estado del sistema queda determinado, al atravesar cada compuerta, por los siguientes 2-qubits:

$$q' = \text{Xor } q = \text{Xor } |x, y\rangle = |x, x \oplus y\rangle$$

$$q'' = \overline{\text{Xor}} q' = \overline{\text{Xor}} |x, x \oplus y\rangle = |x \oplus x \oplus y, x \oplus y\rangle = |0 \oplus y, x \oplus y\rangle = |y, x \oplus y\rangle$$

$$q''' = \text{Xor } q'' = \text{Xor } |y, x \oplus y\rangle = |y, x \oplus y \oplus y\rangle = |y, x \oplus 0\rangle = |y, x\rangle$$

b) El circuito intercambia los qubits de entrada. Suele representarse de forma simplificada del siguiente modo:

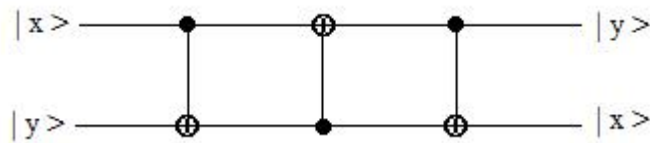
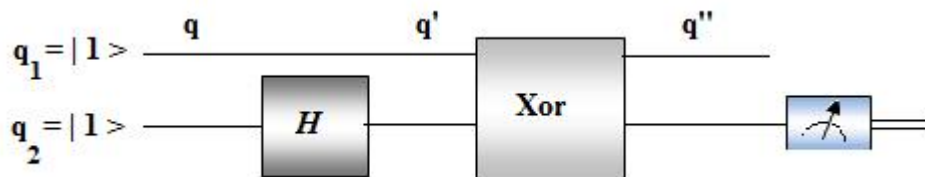


Figura 3.13: Circuito cuántico que intercambia dos qubits

Ejemplo 3.8

Dado el siguiente circuito



- a) Indicar el estado del sistema al atravesar cada compuerta.
b) ¿Quedan entrelazados los qubits al atravesar todas las compuertas?
c) ¿Cuál es la probabilidad de que, al efectuar la medición, el segundo qubit esté en estado 1?
d) ¿En qué estado queda el sistema luego de efectuar la medición del segundo qubit, si éste quedó en estado 0?

Solución

a) Nuevamente, por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema es

$$q = q_1 \otimes q_2 = |1\rangle \otimes |1\rangle = |11\rangle$$

Por otro lado, los otros estados que resultan al atravesar cada compuerta son:

$$q' = q_1 \otimes Hq_2 = |1\rangle \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right) = \frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$q'' = X \text{ or } q' = X \text{ or } \left(\frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle \right) = \frac{1}{\sqrt{2}}X \text{ or } |10\rangle - \frac{1}{\sqrt{2}}X \text{ or } |11\rangle =$$

$$= \frac{1}{\sqrt{2}}|1, 1 \oplus 0\rangle - \frac{1}{\sqrt{2}}|1, 1 \oplus 1\rangle = \frac{1}{\sqrt{2}}|1, 1\rangle - \frac{1}{\sqrt{2}}|1, 0\rangle$$

b) El estado final del sistema es

$$q'' = \frac{1}{\sqrt{2}}|1, 1\rangle - \frac{1}{\sqrt{2}}|1, 0\rangle = \underbrace{|1\rangle}_{\text{Primer qubit}} \otimes \underbrace{\left(\frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle \right)}_{\text{Segundo qubit}}$$

Los qubits no quedan entrelazados porque q'' se expresa como producto tensorial de dos qubits.

c) Siguiendo el mismo procedimiento que en el Ejemplo 2.12, se tiene

$$P(q_2 = |1\rangle) = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

Luego, la probabilidad de que el segundo qubit esté en estado 1 es 0.5.

d) Por la Proposición 2.25 se tiene que el sistema evoluciona al siguiente estado:

$$q''' = \frac{-\frac{1}{\sqrt{2}}|1, 0\rangle}{\sqrt{\left| -\frac{1}{\sqrt{2}} \right|^2}} = -|1, 0\rangle$$

Este circuito puede representarse también, de manera más simplificada, de la forma que se ilustra a continuación:

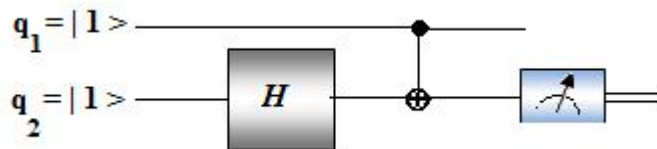
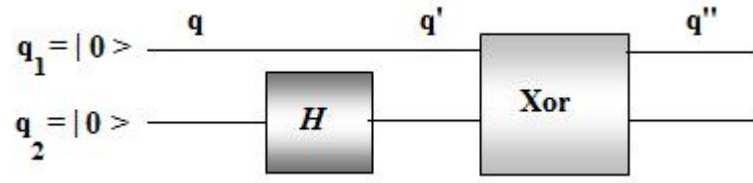


Figura 3.14: Circuito representado en forma simplificada.

El siguiente ejemplo muestra cómo, al modificar los valores de los qubits de entrada, el circuito del ejemplo anterior hace que los qubits queden entrelazados.

Ejemplo 3.9

Dado el siguiente circuito



- Indicar el estado final del sistema.
- Probar que los qubits que componen el sistema quedan entrelazados al atravesar todas las compuertas.

Solución

- Siguiendo los mismos pasos del ejemplo anterior, se prueba que el estado final del sistema es

$$q'' = \frac{1}{\sqrt{2}}|0,0\rangle + \frac{1}{\sqrt{2}}|1,1\rangle$$

- Se supone por el absurdo que los qubits no quedan entrelazados. Luego, el estado final del sistema puede expresarse como producto tensorial de dos qubits. Es decir,

$$q'' = \overline{q_1} \otimes \overline{q_2}$$

Donde

$$\begin{aligned}\overline{q_1} &= \alpha_1 |0\rangle + \beta_1 |1\rangle \\ \overline{q_2} &= \alpha_2 |0\rangle + \beta_2 |1\rangle\end{aligned}$$

Por lo tanto, si $q'' = \overline{q_1} \otimes \overline{q_2}$ entonces

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle$$

De aquí resulta el sistema de ecuaciones

$$\begin{cases} \alpha_1 \alpha_2 = \frac{1}{\sqrt{2}} \\ \alpha_1 \beta_2 = 0 \\ \beta_1 \alpha_2 = 0 \\ \beta_1 \beta_2 = \frac{1}{\sqrt{2}} \end{cases}$$

De la segunda ecuación se tiene que $\alpha_1 = 0$ ó $\beta_2 = 0$.

Si $\alpha_1 = 0$, al reemplazar en la primera ecuación se obtiene $0 = \frac{1}{\sqrt{2}}$.

Similarmente, si $\beta_2 = 0$, al reemplazar en la cuarta ecuación resulta $0 = \frac{1}{\sqrt{2}}$.

En ambos casos se llega a un absurdo, que proviene de suponer que los qubits no están entrelazados.

Compuertas cuánticas de n qubits

Una compuerta cuántica que opera sobre un sistema formado por n qubits es una matriz unitaria de orden 2^n .

Como se mencionó anteriormente, la mayoría de los circuitos cuánticos que operan sobre n qubits se diseñan empleando compuertas de un y dos qubits. Sin embargo, hay dos compuertas importantes que operan sobre un y dos qubits que pueden generalizarse a n qubits: la *compuerta de Hadamard* y la *compuerta f* . Las mismas se aplican en el diseño de la Transformada Cuántica de Fourier. Por esta razón se detallarán a continuación.

La compuerta f para una función booleana de n variables

Dada una función booleana $f : \{0, 1\}^n \rightarrow \{0, 1\}$, la compuerta f es una compuerta de $(n+1)$ qubits definida por

$$U_f |x_1, x_2, \dots, x_n, x_{n+1}\rangle = |x_1, x_2, \dots, x_n, x_{n+1} \oplus f(x_1, x_2, \dots, x_n)\rangle$$

Donde $\oplus$ representa la suma módulo 2 y $x_1, x_2, \dots, x_n, x_{n+1} \in \{0, 1\}$

Su representación gráfica es la siguiente:

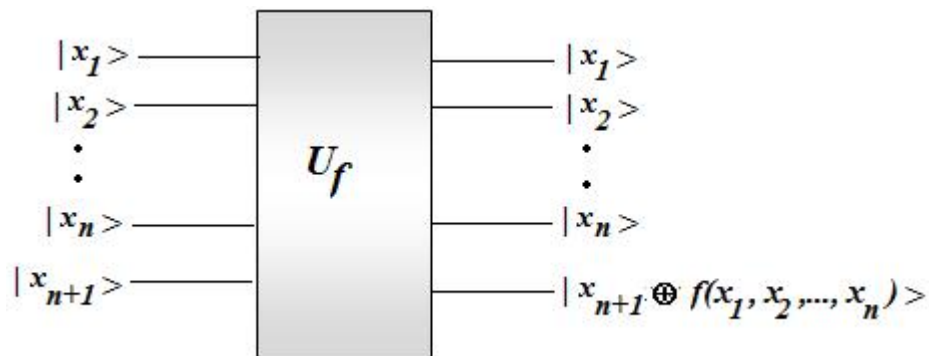
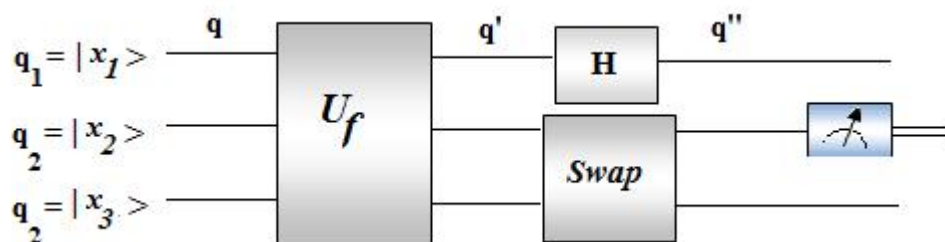


Figura 3.13: Representación gráfica de la compuerta f .

Cabe preguntarse si es factible construir este tipo de compuerta. Se puede afirmar que (véase [5]): “Dado un circuito clásico para calcular f entonces existe un circuito cuántico de eficiencia similar que calcula U_f ”.

Ejemplo 3.10

Dada la función booleana $f : \{0, 1\}^2 \rightarrow \{0, 1\}$ definida por $f(x, y) = x \oplus y$, y el siguiente circuito formado por tres qubits de entrada:



a) Indicar el estado final del sistema.

b) Si $x_1 = 0$, $x_2 = x_3 = 1$ ¿Cuál es la probabilidad de que, al efectuar la medición, el segundo qubit del sistema esté en estado 0?

Solución

a) Por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema es

$$q = q_1 \otimes q_2 \otimes q_3 = |x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle = |x_1 x_2 x_3\rangle$$

Los otros estados que resultan al atravesar cada compuerta son:

$$q' = U_f |x_1, x_2, x_3\rangle = |x_1, x_2, x_3 \oplus f(x_1, x_2)\rangle = |x_1, x_2, x_3 \oplus x_1 \oplus x_2\rangle$$

$$q'' = H |x_1\rangle \otimes \text{Swap} |x_2, x_3 \oplus x_1 \oplus x_2\rangle = H |x_1\rangle \otimes |x_3 \oplus x_1 \oplus x_2, x_2\rangle$$

b) Si $x_1 = 0$, $x_2 = x_3 = 1$ entonces el estado final del sistema es

$$q'' = H |x_1\rangle \otimes |x_3 \oplus x_1 \oplus x_2, x_2\rangle = H |0\rangle \otimes |1 \oplus 0 \oplus 1, 1\rangle = H |0\rangle \otimes |0, 1\rangle =$$

$$= H |0\rangle \otimes |0, 1\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \otimes |0, 1\rangle = \frac{1}{\sqrt{2}}|0 0 1\rangle + \frac{1}{\sqrt{2}}|1 0 1\rangle$$

Por lo tanto,

$$q'' = \frac{1}{\sqrt{2}}|0 0 1\rangle + \frac{1}{\sqrt{2}}|1 0 1\rangle$$

En este caso, la probabilidad de que el segundo qubit esté en estado 0 es

$$P(q_2 = |0\rangle) = \left| \frac{1}{\sqrt{2}} \right|^2 + \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2} + \frac{1}{2} = 1$$

Luego, hay un 100% de seguridad de que el segundo qubit, al medirse, esté en estado 0.

La compuerta de Hadamard para un sistema de n qubits

Se la define por

$$H^{\otimes n} |x_{n-1}, x_{n-2}, \dots, x_0\rangle = H |x_{n-1}\rangle \otimes H |x_{n-2}\rangle \dots \otimes H |x_0\rangle$$

$$\text{Donde } x_0, x_1, \dots, x_{n-1} \in \{0, 1\} \text{ y } H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

La compuerta de Hadamard de n qubits puede expresarse de una manera más sencilla si se utiliza la notación decimal de los qubits de la base. La siguiente Proposición indica cómo es dicha expresión.

Proposición 3.11

Si $n \in \mathbb{N} \wedge x_0, x_1, \dots, x_{n-1} \in \{0, 1\}$ entonces

$$H^{\otimes n} |x_{n-1} x_{n-2} \dots x_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |y\rangle$$

Donde $|y\rangle$ es la expresión en base 10 del n qubit $|y_{n-1} y_{n-2} \dots y_1 y_0\rangle$. Es decir,

$$|y\rangle = \left| \sum_{i=0}^{n-1} y_i 2^i \right\rangle$$

Demostración

Se aplicará el Principio de Inducción sobre n .

Para $n=1$

En este caso, $H^{\otimes 1} |x_0\rangle = H |x_0\rangle$, $x_0 \in \{0, 1\}$ e $y = y_0$. Se consideran dos casos:

1) Si $x_0 = 0$ entonces

$$H^{\otimes 1} |x_0\rangle = H |0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

Por otro lado,

$$\frac{1}{\sqrt{2^1}} \sum_{y=0}^{2^1-1} (-1)^{x_0 \cdot y_0} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^1 (-1)^{0 \cdot y_0} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^1 |y\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

2) Si $x_0 = 1$ entonces

$$H^{\otimes 1} |x_0\rangle = H |1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Por otro lado,

$$\frac{1}{\sqrt{2^1}} \sum_{y=0}^{2^1-1} (-1)^{x_0 \cdot y_0} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^1 (-1)^{1 \cdot y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^1 (-1)^y |y\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

En consecuencia, se verifica que $H^{\otimes 1} |x_0\rangle = \frac{1}{\sqrt{2^1}} \sum_{y=0}^{2^1-1} (-1)^{x_0 \cdot y_0} |y\rangle$

Se supone que la expresión es válida para n (Hipótesis Inductiva).

Es decir,

$$H^{\otimes n} |x_{n-1} x_{n-2} \dots x_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |y\rangle$$

Donde $|y\rangle$ es la expresión en base 10 del n qubit $|y_{n-1} y_{n-2} \dots y_1 y_0\rangle$.

Se probará que la afirmación es válida para (n+1)

O sea, se verificará que

$$H^{\otimes(n+1)} |x_n x_{n-1} x_{n-2} \dots x_0\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^{n+1}-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle$$

Donde $|y\rangle$ es la expresión en base 10 del (n+1) qubit $|y_n y_{n-1} \dots y_1 y_0\rangle$.

Aplicando la definición de la compuerta H para (n+1) qubits y la Hipótesis Inductiva se tiene

$$\begin{aligned} H^{\otimes(n+1)} |x_n x_{n-1} x_{n-2} \dots x_1 x_0\rangle &= H |x_n\rangle \otimes H^{\otimes n} |x_{n-1} x_{n-2} \dots x_1 x_0\rangle = \\ &= H |x_n\rangle \otimes \underbrace{\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |y\rangle}_{\text{Hipótesis Inductiva}} \end{aligned}$$

Luego

$$H^{\otimes(n+1)} |x_n x_{n-1} x_{n-2} \dots x_1 x_0\rangle = H |x_n\rangle \otimes \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |y\rangle \quad [1]$$

Se consideran dos casos:

Primer Caso: $x_n = 0$

Reemplazando en [1] se obtiene

$$\begin{aligned} H^{\otimes(n+1)} |x_n x_{n-1} x_{n-2} \dots x_1 x_0\rangle &= H |0\rangle \otimes \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |y\rangle = \\ &= \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |y\rangle = \end{aligned}$$

$$\begin{aligned}
& \left(\frac{1}{\sqrt{2}} |0\rangle \otimes \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |y\rangle \right) + \left(\frac{1}{\sqrt{2}} |1\rangle \otimes \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |y\rangle \right) = \\
& = \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |0\rangle \otimes |y\rangle \right) + \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |1\rangle \otimes |y\rangle \right) = \\
& = \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |0\rangle \otimes |y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right) + \\
& + \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}} |1\rangle \otimes |y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right) = \\
& = \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1} + x_n \cdot 0} |0 y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right) + \\
& + \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1} + x_n \cdot 1} |1 y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right)
\end{aligned}$$

En consecuencia, teniendo en cuenta que $y_n = \begin{cases} 0 & \text{para } 0 y_{n-1} y_{n-2} \dots y_1 y_0 \\ 1 & \text{para } 1 y_{n-1} y_{n-2} \dots y_1 y_0 \end{cases}$ se tiene

$$\begin{aligned}
H^{\otimes(n+1)} |x_n x_{n-1} x_{n-2} \dots x_1 x_0\rangle &= \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |0 y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right) + \\
& + \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |1 y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right) \quad [2]
\end{aligned}$$

En la primera sumatoria del miembro derecho de la ecuación [2], la expresión en base 10 del dígito binario $0 y_{n-1} y_{n-2} \dots y_1 y_0$ es

$$0 \cdot 2^n + \sum_{i=0}^{n-1} y_i 2^i = 0 + y = y$$

Por lo tanto

$$|0 y_{n-1} y_{n-2} \dots y_1 y_0\rangle = |y\rangle$$

Luego

$$\left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |0 y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right) = \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle \right) \quad [3]$$

Por otro lado, en la segunda sumatoria del miembro derecho de la ecuación [2], la expresión en base 10 del dígito binario $1 y_{n-1} y_{n-2} \dots y_1 y_0$ es

$$1 \cdot 2^n + \sum_{i=0}^{n-1} y_i 2^i = 2^n + y$$

Por lo tanto

$$|1 y_{n-1} y_{n-2} \dots y_1 y_0\rangle = |2^n + y\rangle$$

Luego

$$\begin{aligned} \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |1 y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right) &= \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |2^n + y\rangle \right) = \\ &= \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=2^n}^{2^n+2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle \right) = \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=2^n}^{2^{n+1}-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle \right) \end{aligned}$$

De aquí se obtiene

$$\left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |1 y_{n-1} y_{n-2} \dots y_1 y_0\rangle \right) = \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=2^n}^{2^{n+1}-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle \right) \quad [4]$$

Reemplazando [3] y [4] en [2] resulta

$$\begin{aligned} H^{\otimes(n+1)} |x_n x_{n-1} x_{n-2} \dots x_1 x_0\rangle &= \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle \right) + \\ &+ \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=2^n}^{2^{n+1}-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle \right) = \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^{n+1}-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle \end{aligned}$$

En consecuencia,

$$H^{\otimes(n+1)} |x_n x_{n-1} x_{n-2} \dots x_1 x_0\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^{n+1}-1} (-1)^{x_0 \cdot y_0 + \dots + x_n \cdot y_n} |y\rangle$$

Segundo Caso: $x_n = 1$

Se resuelve de manera similar al Primer Caso. ■

Notación 3.12

Teniendo en cuenta que $x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}$ es el producto escalar de los vectores $x = (x_{n-1}, x_{n-2}, \dots, x_0)$ e $y = (y_{n-1}, y_{n-2}, \dots, y_0)$, la fórmula de la compuerta de Hadamard obtenida en la Proposición 3.11 puede compactarse del siguiente modo:

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

Donde $|x\rangle = |x_{n-1}, x_{n-2}, \dots, x_0\rangle$ $\wedge$ $x \cdot y = x_0 \cdot y_0 + \dots + x_{n-1} \cdot y_{n-1}$.

Ejemplo 3.13

1) Aplicar la Proposición 3.11 para hallar la expresión de la compuerta de Hadamard para un sistema de 3 qubits.

2) Calcular $H^{\otimes 3} |100\rangle$

Solución

1) De la Proposición 3.11 se tiene que

$$H^{\otimes 3} |x_2 x_1 x_0\rangle = \frac{1}{\sqrt{2^3}} \sum_{y=0}^{2^3-1} (-1)^{x_0 \cdot y_0 + x_1 \cdot y_1 + x_2 \cdot y_2} |y\rangle = \frac{1}{\sqrt{2^3}} \sum_{y=0}^7 (-1)^{x_0 \cdot y_0 + x_1 \cdot y_1 + x_2 \cdot y_2} |y\rangle \quad [1]$$

Donde $|y\rangle$ es la expresión en base 10 del 3 qubit $|y_2 y_1 y_0\rangle$.

En el siguiente cuadro se muestra la correspondencia entre el número “y” y su expresión en binario:

y	$y_2 y_1 y_0$
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Sustituyendo estos datos de la tabla en [1] se obtiene

$$H^{\otimes 3} |x_2 x_1 x_0\rangle = \frac{1}{\sqrt{2^3}} \left((-1)^0 |0\rangle + (-1)^{x_0} |1\rangle + (-1)^{x_1} |2\rangle + (-1)^{x_0 + x_1} |3\rangle + (-1)^{x_2} |4\rangle + \right. \\ \left. + (-1)^{x_0 + x_2} |5\rangle + (-1)^{x_1 + x_2} |6\rangle + (-1)^{x_0 + x_1 + x_2} |7\rangle \right)$$

Es decir,

$$H^{\otimes 3} |x_2 x_1 x_0\rangle = \frac{1}{\sqrt{2^3}} \left(|000\rangle + (-1)^{x_0} |001\rangle + (-1)^{x_1} |010\rangle + (-1)^{x_0+x_1} |011\rangle + (-1)^{x_2} |100\rangle + (-1)^{x_0+x_2} |101\rangle + (-1)^{x_1+x_2} |110\rangle + (-1)^{x_0+x_1+x_2} |111\rangle \right)$$

2) En este caso, $x_0 = x_1 = 0$, $x_2 = 1$. Por lo tanto, del inciso 1) resulta

$$H^{\otimes 3} |100\rangle = \frac{1}{\sqrt{2^3}} (|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle)$$

En el próximo capítulo se desarrollarán algunos algoritmos cuánticos más conocidos. Esto permitirá comprender el funcionamiento de un computador cuántico para luego manipular e interpretar los resultados que arroja un algoritmo.

Capítulo 4

Algunos Algoritmos cuánticos

Un algoritmo es un conjunto de instrucciones que se utilizan para realizar una determinada tarea en una computadora.

Gran parte del deseo de desarrollar una computadora cuántica proviene del descubrimiento de que algunos algoritmos funcionan drásticamente mejor en una computadora cuántica de lo que podrían trabajar en un ordenador clásico.

Ello se debe a una importante característica que gozan los sistemas cuánticos: *el paralelismo cuántico*.

El paralelismo cuántico es la propiedad que tienen los algoritmos cuánticos de efectuar varias operaciones al mismo tiempo, en virtud del estado de superposición que pueden adquirir las partículas subatómicas.

Gracias a ello, las computadoras cuánticas pueden valuar, en forma simultánea, una función $f(x)$ para múltiples valores de x .

Sin embargo, se sabe que, al medir un qubit, éste colapsa a uno de los dos estados posibles: estado 0 (spin arriba) o estado 1 (spin abajo).

¿Dónde está, pues, la ventaja de utilizar algoritmos cuánticos? La ventaja radica en que se pueden manipular los qubits a través de compuertas cuánticas sin que colapsen sus estados. Así, se pueden manejar qubits en estado de superposición y en el momento apropiado, observarlos. En ese instante sus estados colapsarán, pero antes de ello sus estados darán la información necesaria para los propósitos del algoritmo.

En la actualidad han sido creados sólo un pequeño conjunto de algoritmos cuánticos, y sigue siendo un área de investigación muy activa.

En este capítulo se desarrollarán algunos de los más importantes:

- El Algoritmo de Deutsch.
- El Algoritmo de Deutsch- Josza.
- El Algoritmo de Simon

El Algoritmo de Deutsch

Fue uno de los primeros algoritmos cuánticos. Ideado por David Deutsch en 1985, su finalidad es determinar si una función booleana de una variable $f : \{0,1\} \rightarrow \{0,1\}$ es constante o no.

Aunque no sea de gran utilidad para casos prácticos, en él se empieza a apreciar el funcionamiento y la potencia de los programas cuánticos. Antes de explicar el algoritmo, se precisarán ciertos conceptos previos que se mencionarán a continuación.

Nociones previas

Definición 4.1: Complemento de una función booleana

Dada una función booleana de una variable $f : \{0,1\} \rightarrow \{0,1\}$, su complemento es

$$\overline{f(x)} = \begin{cases} 1 & \text{si } f(x) = 0 \\ 0 & \text{si } f(x) = 1 \end{cases}$$

De la definición anterior se deduce que si $x \in \{0,1\}$ entonces

$$\begin{cases} 1 \oplus f(x) = \overline{f(x)} \\ 0 \oplus f(x) = f(x) \end{cases}$$

Donde $\oplus$ es la suma módulo 2.

La siguiente Proposición será aplicada en el desarrollo del algoritmo.

Proposición 4.2

Dada una función booleana de una variable $f : \{0,1\} \rightarrow \{0,1\}$, si $x \in \{0,1\}$ entonces

$$|f(x)\rangle - |\overline{f(x)}\rangle = (-1)^{f(x)} (|0\rangle - |1\rangle)$$

Demostración

Si $f(x) = 0$ entonces

$$|f(x)\rangle - |\overline{f(x)}\rangle = |0\rangle - |1\rangle = (-1)^{f(x)} (|0\rangle - |1\rangle)$$

Por otro lado, si $f(x) = 1$ entonces

$$|f(x)\rangle - |\overline{f(x)}\rangle = |1\rangle - |0\rangle = (-1)(|0\rangle - |1\rangle) = (-1)^{f(x)} (|0\rangle - |1\rangle) \blacksquare$$

Descripción del Algoritmo de Deutsch

Como se mencionó anteriormente, dada una función booleana $f : \{0,1\} \rightarrow \{0,1\}$, el algoritmo cuántico de Deutsch determinará si $f(x)$ es constante o no. El circuito cuántico que implementa el algoritmo tiene dos entradas: $q_1 = |0\rangle$ y $q_2 = |1\rangle$. Se lo muestra a continuación:

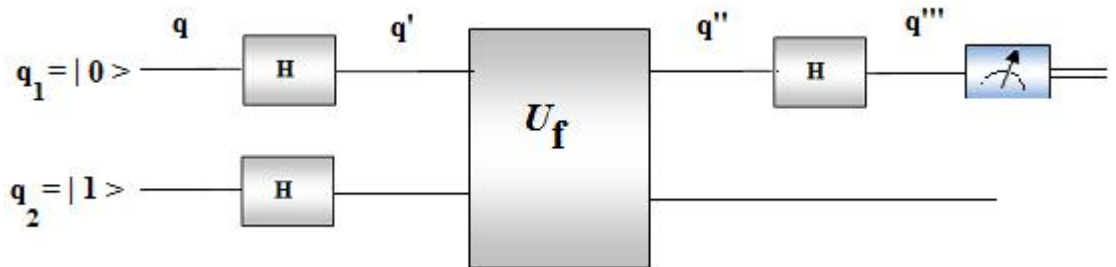


Figura 4.1: Circuito cuántico del algoritmo de Deutsch.

Se analizarán los distintos estados del sistema al atravesar cada compuerta, para finalmente llegar al estado final. Por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema es

$$q = q_1 \otimes q_2 = |0\rangle \otimes |1\rangle = |01\rangle$$

Los otros estados resultantes son:

$$\begin{aligned} q' &= H|0\rangle \otimes H|1\rangle = \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) = \\ &= \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{aligned}$$

Al atravesar la compuerta f se tendrá en cuenta que ésta representa una transformación lineal y, al aplicar la Proposición 4.2 se obtiene:

$$\begin{aligned} q'' &= U_f q' = U_f \left(\frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) \right) = \\ &= \frac{1}{2} U_f (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2} (U_f(|00\rangle) - U_f(|01\rangle) + U_f(|10\rangle) - U_f(|11\rangle)) = \\ &= \frac{1}{2} (|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle) = \\ &= \frac{1}{2} (|0, f(0)\rangle - |0, \overline{f(0)}\rangle + |1, f(1)\rangle - |1, \overline{f(1)}\rangle) = \\ &= \frac{1}{2} (|0\rangle \otimes |f(0)\rangle - |0\rangle \otimes |\overline{f(0)}\rangle + |1\rangle \otimes |f(1)\rangle - |1\rangle \otimes |\overline{f(1)}\rangle) = \\ &= \frac{1}{2} (|0\rangle \otimes (|f(0)\rangle - |\overline{f(0)}\rangle) + |1\rangle \otimes (|f(1)\rangle - |\overline{f(1)}\rangle)) = \\ &= \frac{1}{2} (|0\rangle \otimes (-1)^{f(0)} (|0\rangle - |1\rangle) + |1\rangle \otimes (-1)^{f(1)} (|0\rangle - |1\rangle)) = \\ &= \frac{1}{2} ((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle) \otimes (|0\rangle - |1\rangle) = \\ &= \frac{1}{\sqrt{2}} ((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\ &= \left(\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) \end{aligned}$$

Por lo tanto

$$q'' = \underbrace{\left(\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}} |1\rangle \right)}_{\text{Primer qubit}} \otimes \underbrace{\left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right)}_{\text{Segundo qubit}}$$

Se observa que el primer qubit del sistema está en estado de superposición, y contiene simultáneamente los valores $f(0)$ y $f(1)$. Es aquí donde se destaca el paralelismo cuántico, ya que se está almacenando al mismo tiempo $f(0)$ y $f(1)$, que son todos los valores que toma la función f . Por esta razón se dice que el Algoritmo de Deutsch es como “mirar a la vez las dos caras de una moneda”.

Por último, el estado final del sistema es

$$q''' = H \left(\underbrace{\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}} |1\rangle}_{\text{Primer qubit}} \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) \quad [1]$$

Como se verá a continuación, el primer qubit del sistema determinará si la función es o no constante. Al aplicarle la compuerta de Hadamard se obtiene:

$$\begin{aligned} H \left(\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}} |1\rangle \right) &= \frac{(-1)^{f(0)}}{\sqrt{2}} H |0\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}} H |1\rangle = \\ &= \frac{(-1)^{f(0)}}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) + \frac{(-1)^{f(1)}}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) = \\ &= \left(\frac{(-1)^{f(0)} + (-1)^{f(1)}}{2} \right) |0\rangle + \left(\frac{(-1)^{f(0)} - (-1)^{f(1)}}{2} \right) |1\rangle \end{aligned}$$

Por lo tanto

$$H \left(\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}} |1\rangle \right) = \left(\frac{(-1)^{f(0)} + (-1)^{f(1)}}{2} \right) |0\rangle + \left(\frac{(-1)^{f(0)} - (-1)^{f(1)}}{2} \right) |1\rangle \quad [2]$$

Sustituyendo [2] en [1] y aplicando la Proposición 1.9 inciso 3), se obtiene que el estado final del sistema es

$$q''' = \left(\underbrace{\left(\frac{(-1)^{f(0)} + (-1)^{f(1)}}{2} \right) |0\rangle + \left(\frac{(-1)^{f(0)} - (-1)^{f(1)}}{2} \right) |1\rangle}_{\text{Primer qubit } q_1} \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right)$$

Por lo tanto, si se efectúa la medición del primer qubit del sistema resulta:

1) Si f es constante, el primer qubit estará en estado 0 con probabilidad 1 pues:

$$P(q_1 = |0\rangle) = \left| \frac{(-1)^{f(0)} + (-1)^{f(1)}}{2} \right|^2 = \left| \frac{1}{2} (\pm 2) \right|^2 = 1$$

2) Si f no es constante, el primer qubit estará en estado 1 con probabilidad 1 pues:

$$P(q_1 = |1\rangle) = \left| \frac{(-1)^{f(0)} - (-1)^{f(1)}}{2} \right|^2 = \left| \frac{1}{2} (\pm 2) \right|^2 = 1$$

Observación 4.3

En un algoritmo computacional clásico, para verificar si una función booleana de una variable f es constante o no, es preciso valuar si $f(0) = f(1)$. En cambio, en el Algoritmo de Deutsch esta valuación no es necesaria, ya que basta que la compuerta f cargue simultáneamente todos los valores de la función para determinar si es o no constante. Sin embargo, el Algoritmo de Deutsch no brinda demasiada ventaja en relación a un algoritmo computacional clásico. Pero para funciones booleanas de varias variables, el Algoritmo de Deutsch-Josza que se expondrá a continuación, muestra una eficiencia notablemente mejor que cualquier otro algoritmo clásico que permita determinar si una función booleana de varias variables es constante o balanceada.

El Algoritmo de Deutsch-Josza

Este algoritmo es una generalización del Algoritmo de Deutsch. Fue ideado en 1992 por David Deutsch y Richard Josza y muestra claramente la superioridad de las computadoras cuánticas sobre las clásicas.

En el problema de Deutsch-Josza se da una función booleana $f(x_1, x_2, \dots, x_n)$ (como si estuviera contenida en una caja negra) y de ella se informa que puede ser constante o bien balanceada (es decir, toma el valor 1 para la mitad de las entradas y 0 para la otra mitad). El Algoritmo consiste en determinar cómo es la función (constante o balanceada). El siguiente ejemplo ilustra la definición de función balanceada.

Ejemplo 4.4

Dada la función booleana $f : \{0, 1\}^2 \rightarrow \{0, 1\}$ definida por

$$\begin{cases} f(0,0)=0 \\ f(0,1)=1 \\ f(1,0)=0 \\ f(1,1)=1 \end{cases}$$

Entonces f es balanceada pues toma el valor 1 la misma cantidad de veces que el valor 0.

En el desarrollo del algoritmo se utilizarán los siguientes conceptos, que son una extensión de la Definición 4.1 y de la Proposición 4.2

Definición 4.5: Complemento de una función booleana de n variables

Dada una función booleana de n variables $f : \{0, 1\}^n \rightarrow \{0, 1\}$, su complemento es

$$\overline{f(x_1, x_2, \dots, x_n)} = \begin{cases} 1 & \text{si } f(x_1, x_2, \dots, x_n) = 0 \\ 0 & \text{si } f(x_1, x_2, \dots, x_n) = 1 \end{cases}$$

De la definición anterior se deduce que si $x_1, x_2, \dots, x_n \in \{0, 1\}$ entonces

$$\begin{aligned} 1 \oplus f(x_1, x_2, \dots, x_n) &= \overline{f(x_1, x_2, \dots, x_n)} \\ 0 \oplus f(x_1, x_2, \dots, x_n) &= f(x_1, x_2, \dots, x_n) \end{aligned}$$

Proposición 4.6

Sea $f : \{0,1\}^n \rightarrow \{0,1\}$ una función booleana de n variables.

Si $x_1, x_2, \dots, x_n \in \{0,1\}$ entonces

$$\left| f(x_1, x_2, \dots, x_n) \right\rangle - \left| \overline{f(x_1, x_2, \dots, x_n)} \right\rangle = (-1)^{f(x_1, x_2, \dots, x_n)} (|0\rangle - |1\rangle)$$

Demostración

Es similar a la Proposición 4.2. ■

Por cuestiones didácticas se explicará el algoritmo de Deutsch-Josza para funciones booleanas de dos variables, para luego extenderlo a n variables.

Algoritmo de Deutsch-Josza para funciones booleanas de dos variables

Dada una función booleana $f : \{0,1\}^2 \rightarrow \{0,1\}$, el algoritmo cuántico de Deutsch-Josza determinará si f es constante o balanceada. El circuito cuántico que implementa el algoritmo tiene tres entradas: $q_1 = |0\rangle$, $q_2 = |0\rangle$ y $q_3 = |1\rangle$ y es el siguiente:

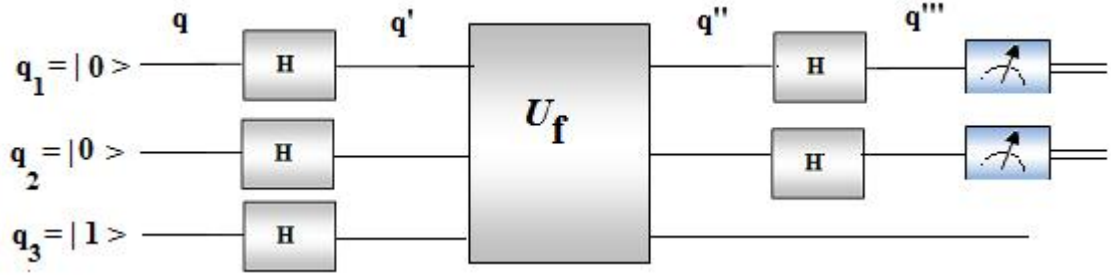


Figura 4.2: Circuito cuántico del algoritmo de Deutsch-Josza para una función booleana de dos variables.

Nuevamente, se analizarán los distintos estados del sistema al atravesar cada compuerta, para finalmente llegar al estado final. Por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema es

$$q = q_1 \otimes q_2 \otimes q_3 = |0\rangle \otimes |0\rangle \otimes |1\rangle = |001\rangle$$

Los otros estados resultantes son:

$$\begin{aligned} q' &= H|0\rangle \otimes H|0\rangle \otimes H|1\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right) = \\ &= \frac{1}{\sqrt{2^3}} (|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle) \end{aligned}$$

Al atravesar la compuerta f y aplicar la Definición 4.5 y la Proposición 4.6 se obtiene:

$$q'' = U_f q' = U_f \left(\frac{1}{\sqrt{2^3}} (|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle) \right) =$$

$$\begin{aligned}
&= \frac{1}{\sqrt{2^3}} (U_f |000\rangle - U_f |001\rangle + U_f |010\rangle - U_f |011\rangle + U_f |100\rangle - U_f |101\rangle + U_f |110\rangle - U_f |111\rangle) = \\
&= \frac{1}{\sqrt{2^3}} (|0,0,0 \oplus f(0,0)\rangle - |0,0,1 \oplus f(0,0)\rangle + |0,1,0 \oplus f(0,1)\rangle - |0,1,1 \oplus f(0,1)\rangle + \\
&+ |1,0,0 \oplus f(1,0)\rangle - |1,0,1 \oplus f(1,0)\rangle + |1,1,0 \oplus f(1,1)\rangle - |1,1,1 \oplus f(1,1)\rangle) = \\
&= \frac{1}{\sqrt{2^3}} (|0,0,f(0,0)\rangle - |0,0,\overline{f(0,0)}\rangle + |0,1,f(0,1)\rangle - |0,1,\overline{f(0,1)}\rangle + \\
&+ |1,0,f(1,0)\rangle - |1,0,\overline{f(1,0)}\rangle + |1,1,f(1,1)\rangle - |1,1,\overline{f(1,1)}\rangle) = \\
&= \frac{1}{\sqrt{2^3}} (|00\rangle \otimes |f(0,0)\rangle - |00\rangle \otimes |\overline{f(0,0)}\rangle + |01\rangle \otimes |f(0,1)\rangle - |01\rangle \otimes |\overline{f(0,1)}\rangle + \\
&+ |10\rangle \otimes |f(1,0)\rangle - |10\rangle \otimes |\overline{f(1,0)}\rangle + |11\rangle \otimes |f(1,1)\rangle - |11\rangle \otimes |\overline{f(1,1)}\rangle) = \\
&= \frac{1}{\sqrt{2^3}} (|00\rangle \otimes (|f(0,0)\rangle - |\overline{f(0,0)}\rangle) + |01\rangle \otimes (|f(0,1)\rangle - |\overline{f(0,1)}\rangle) + \\
&+ |10\rangle \otimes (|f(1,0)\rangle - |\overline{f(1,0)}\rangle) + |11\rangle \otimes (|f(1,1)\rangle - |\overline{f(1,1)}\rangle)) = \\
&= \frac{1}{\sqrt{2^3}} (|00\rangle \otimes (-1)^{f(0,0)} (|0\rangle - |1\rangle) + |01\rangle \otimes (-1)^{f(0,1)} (|0\rangle - |1\rangle) + \\
&+ |10\rangle \otimes (-1)^{f(1,0)} (|0\rangle - |1\rangle) + |11\rangle \otimes (-1)^{f(1,1)} (|0\rangle - |1\rangle)) = \\
&= \frac{1}{\sqrt{2^3}} \left(\left((-1)^{f(0,0)} |00\rangle + (-1)^{f(0,1)} |01\rangle + (-1)^{f(1,0)} |10\rangle + (-1)^{f(1,1)} |11\rangle \right) \otimes (|0\rangle - |1\rangle) \right)
\end{aligned}$$

Por lo tanto

$$q'' = \frac{1}{\sqrt{2^3}} \left(\left((-1)^{f(0,0)} |00\rangle + (-1)^{f(0,1)} |01\rangle + (-1)^{f(1,0)} |10\rangle + (-1)^{f(1,1)} |11\rangle \right) \otimes (|0\rangle - |1\rangle) \right)$$

O equivalentemente

$$q'' = \frac{1}{\sqrt{2^2}} \left(\left((-1)^{f(0,0)} |00\rangle + (-1)^{f(0,1)} |01\rangle + (-1)^{f(1,0)} |10\rangle + (-1)^{f(1,1)} |11\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$$

Es decir,

$$q'' = \frac{1}{2} \left(\left((-1)^{f(0,0)} |00\rangle + (-1)^{f(0,1)} |01\rangle + (-1)^{f(1,0)} |10\rangle + (-1)^{f(1,1)} |11\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$$

Estado de los dos primeros qubits del sistema

Al aplicar la compuerta de Hadamard a los dos primeros qubits del sistema, se obtiene el estado final

$$q''' = H^{\otimes 2} \left(\underbrace{\frac{1}{2} \left((-1)^{f(0,0)} |00\rangle + (-1)^{f(0,1)} |01\rangle + (-1)^{f(1,0)} |10\rangle + (-1)^{f(1,1)} |11\rangle \right)}_{\text{Estado de los dos primeros qubits del sistema}} \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Se probará que los dos primeros qubits del sistema determinarán si la función es constante o balanceada. Al aplicarle la compuerta de Hadamard se obtiene:

$$\begin{aligned} H^{\otimes 2} \left(\frac{1}{2} \left((-1)^{f(0,0)} |00\rangle + (-1)^{f(0,1)} |01\rangle + (-1)^{f(1,0)} |10\rangle + (-1)^{f(1,1)} |11\rangle \right) \right) &= \\ = \frac{1}{2} \left((-1)^{f(0,0)} H^{\otimes 2} |00\rangle + (-1)^{f(0,1)} H^{\otimes 2} |01\rangle + (-1)^{f(1,0)} H^{\otimes 2} |10\rangle + (-1)^{f(1,1)} H^{\otimes 2} |11\rangle \right) &= \\ = \frac{1}{2} \left((-1)^{f(0,0)} H |0\rangle \otimes H |0\rangle + (-1)^{f(0,1)} H |0\rangle \otimes H |1\rangle + (-1)^{f(1,0)} H |1\rangle \otimes H |0\rangle + (-1)^{f(1,1)} H |1\rangle \otimes H |1\rangle \right) &= \end{aligned}$$

Desarrollando la compuerta de Hadamard en cada término resulta

$$\begin{aligned} &= \frac{1}{4} \left((-1)^{f(0,0)} + (-1)^{f(0,1)} + (-1)^{f(1,0)} + (-1)^{f(1,1)} \right) |00\rangle + \\ &\frac{1}{4} \left((-1)^{f(0,0)} - (-1)^{f(0,1)} + (-1)^{f(1,0)} - (-1)^{f(1,1)} \right) |01\rangle + \\ &\frac{1}{4} \left((-1)^{f(0,0)} + (-1)^{f(0,1)} - (-1)^{f(1,0)} - (-1)^{f(1,1)} \right) |10\rangle + \\ &\frac{1}{4} \left((-1)^{f(0,0)} - (-1)^{f(0,1)} - (-1)^{f(1,0)} + (-1)^{f(1,1)} \right) |11\rangle = \\ &= \begin{cases} \pm |00\rangle & \text{si } f(0,0) = f(0,1) = f(1,0) = f(1,1) \\ \pm |10\rangle & \text{si } f(0,0) = f(0,1) \wedge f(1,0) = f(1,1) \wedge f \neq \text{cte} \\ \pm |01\rangle & \text{si } f(0,0) = f(1,0) \wedge f(0,1) = f(1,1) \wedge f \neq \text{cte} \\ \pm |11\rangle & \text{si } f(0,0) = f(1,1) \wedge f(0,1) = f(1,0) \wedge f \neq \text{cte} \end{cases} \end{aligned}$$

Por lo tanto, si se efectúa la medición de los dos primeros qubits del sistema resulta:

1) Si f es constante, los dos primeros qubits estarán en estado 0 con probabilidad 1 pues:

$$P(q_1 = |0\rangle \wedge q_2 = |0\rangle) = \left| \frac{1}{4} \left((-1)^{f(0,0)} + (-1)^{f(0,1)} + (-1)^{f(1,0)} + (-1)^{f(1,1)} \right) \right|^2 = \left| \frac{1}{4} (\pm 4) \right|^2 = 1$$

2) Si f está balanceada, ambos qubits estarán en estado 0 con probabilidad 0 pues:

$$P(q_1 = |0\rangle \wedge q_2 = |0\rangle) = \left| \frac{1}{4} \left((-1)^{f(0,0)} + (-1)^{f(0,1)} + (-1)^{f(1,0)} + (-1)^{f(1,1)} \right) \right|^2 = \left| \frac{1}{4} (0) \right|^2 = 0$$

A continuación se procederá a la generalización del Algoritmo de Deutsch-Josza para funciones booleanas de n variables.

Algoritmo de Deutsch-Josza para funciones booleanas de n variables

Dada una función booleana $f : \{0,1\}^n \rightarrow \{0,1\}$, el algoritmo cuántico de Deutsch - Josza determinará si f es constante o balanceada. El circuito cuántico que implementa el algoritmo tiene $(n+1)$ entradas: $q_1 = q_2 = \dots = q_n = |0\rangle \wedge q_{n+1} = |1\rangle$ y es el siguiente:

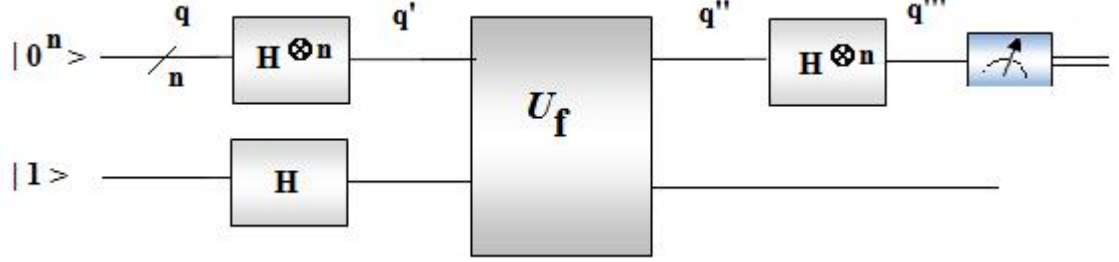


Figura 4.3: Circuito cuántico del algoritmo de Deutsch.-Josza para una función booleana de n variables.

En este caso, $|0^n\rangle$ representa el n -qubit $|00\dots0\rangle$, el cual contiene n ceros. El estado inicial del sistema es

$$q = q_1 \otimes q_2 \otimes \dots \otimes q_n \otimes q_{n+1} = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |1\rangle = |00\dots01\rangle = |00\dots0\rangle \otimes |1\rangle$$

Considerando la expresión decimal de los n qubits del sistema y haciendo uso de las Proposiciones 3.11, la Notación 3.12 y la Proposición 4.6, los otros estados resultantes son:

$$\begin{aligned} q' &= H^{\otimes n} |00\dots0\rangle \otimes H |1\rangle = H^{\otimes n} |0\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{0 \cdot x} |x\rangle \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) = \\ &= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \right) \otimes (|0\rangle - |1\rangle) \end{aligned}$$

Es decir,

$$q' = \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \right) \otimes (|0\rangle - |1\rangle)$$

Al atravesar la compuerta f el sistema evoluciona al siguiente estado:

$$\begin{aligned} q'' &= U_f q' = U_f \left(\frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \right) \otimes (|0\rangle - |1\rangle) \right) = U_f \left(\frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle - \sum_{x=0}^{2^n-1} |x\rangle \otimes |1\rangle \right) \right) = \\ &= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} U_f (|x\rangle \otimes |0\rangle) - \sum_{x=0}^{2^n-1} U_f (|x\rangle \otimes |1\rangle) \right) = \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes |0 \oplus f(x)\rangle - \sum_{x=0}^{2^n-1} |x\rangle \otimes |1 \oplus f(x)\rangle \right) = \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle - \sum_{x=0}^{2^n-1} |x\rangle \otimes |\overline{f(x)}\rangle \right) = \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes (|f(x)\rangle - |\overline{f(x)}\rangle) \right) = \\
&= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes (-1)^{f(x)} (|0\rangle - |1\rangle) \right) = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right) \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)
\end{aligned}$$

Luego

$$q'' = \underbrace{\left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right)}_{\text{Estado de los } n \text{ primeros qubits del sistema}} \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$$

Estado de los n primeros qubits del sistema

Finalmente, al aplicar la compuerta de Hadamard a los n primeros qubits del sistema se tiene:

$$q''' = H^{\otimes n} \underbrace{\left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right)}_{\text{Estado de los } n \text{ primeros qubits.}} \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$$

En este caso, los n primeros qubits del sistema determinarán si la función es constante o balanceada. Desarrollando estos qubits resulta.

$$\begin{aligned}
H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right) &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle = \\
&= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot y} |y\rangle
\end{aligned}$$

Luego

$$H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right) = \sum_{y=0}^{2^n-1} \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot y} |y\rangle$$

Por lo tanto, si se efectúa la medición de los n primeros qubits del sistema resulta:

1) Si f es constante entonces $f(x) = 0 \ \forall x$ ó $f(x) = 1 \ \forall x$. En este caso, los n primeros qubits estarán en estado 0 con probabilidad 1 pues:

$$\begin{aligned}
P(q_1 = |0\rangle \wedge q_2 = |0\rangle \wedge \dots \wedge q_n = |0\rangle) &= P(|y\rangle = |0\rangle) = \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot 0} \right|^2 = \\
&= \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2 = \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} \pm 1 \right|^2 = \left| \frac{\pm 1}{2^n} \sum_{x=0}^{2^n-1} 1 \right|^2 = \left| \frac{\pm 1}{2^n} (2^n) \right|^2 = 1
\end{aligned}$$

2) Si f está balanceada, los n qubits estarán en estado 0 con probabilidad 0 pues:

$$P(q_1 = |0\rangle \wedge q_2 = |0\rangle \wedge \dots \wedge q_n = |0\rangle) = P(|y\rangle = |0\rangle) = \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot 0} \right|^2 =$$

$$= \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2 = \left| \frac{1}{2^n} (0) \right|^2 = 0$$

Los términos se compensan y da 0.

Observación 4.7

1) Si se sabe a priori que una función booleana f de n variables es constante o balanceada, como su dominio contiene 2^n elementos, en el peor de los casos un algoritmo clásico debería evaluar en la mitad más uno de los elementos del dominio para determinar si la función es constante o balanceada. Es decir, tendría que realizar

$$\frac{2^n}{2} + 1 = 2^{n-1} + 1 \text{ evaluaciones.}$$

En cambio, en el Algoritmo de Deutsch-Josza sólo se necesita evaluar f una sola vez. Por esta razón se dice que, en este algoritmo cuántico, hay una ganancia exponencial frente a los algoritmos clásicos.

2) La primera implementación experimental de este algoritmo fue propuesta, para dos qubits, en 1998 por Jonathan Jones y Michele Mosca, empleando técnicas de spins bajo resonancia magnética nuclear.

El Algoritmo de Simon

Este algoritmo, propuesto por Daniel Simon en 1994, fue la inspiración para que Shor creara su algoritmo de factorización de un número primo. Se trata de encontrar el período de una función booleana del tipo $f : \{0,1\}^n \rightarrow \{0,1\}^n$. Antes de desarrollar el algoritmo, se introducirán las siguientes definiciones:

Definición 4.7: Vector booleano

Un vector $x = (x_1, x_2, \dots, x_n)$ es booleano si $x_i \in \{0,1\} \forall i=1,2,\dots,n$

Definición 4.8: Suma booleana de vectores

Si $x = (x_1, x_2, \dots, x_n) \wedge y = (y_1, y_2, \dots, y_n)$, con $x_i, y_i \in \{0,1\} \forall i=1,2,\dots,n$ entonces

$$x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, \dots, x_n \oplus y_n)$$

Donde $\oplus$ es la suma módulo 2.

La siguiente Proposición será utilizada en el desarrollo del Algoritmo de Simon.

Proposición 4.9

1) Si $a, b, c \in \{0, 1\}$ entonces

$$(a \oplus b) \cdot c = (a \cdot c) \oplus (b \cdot c)$$

2) Si $p, q \in \mathbb{Z}_{\geq 0}$ entonces

$$(-1)^{p \oplus q} = (-1)^p \cdot (-1)^q$$

3) Si $x = (x_1, x_2, \dots, x_n)$, $y = (y_1, y_2, \dots, y_n)$, $z = (z_1, z_2, \dots, z_n)$ son vectores booleanos entonces

$$(-1)^{z \cdot (x \oplus y)} = (-1)^{z \cdot x} \cdot (-1)^{z \cdot y}$$

Donde $\cdot$ es el producto interno canónico de vectores.

Demostración

1) Se elabora la siguiente tabla con los posibles valores de a , b y c :

a	b	c	$(a \oplus b) \cdot c$	$(a \cdot c) \oplus (b \cdot c)$
0	0	0	$(0 \oplus 0) \cdot 0 = 0$	$(0 \cdot 0) \oplus (0 \cdot 0) = 0$
0	0	1	$(0 \oplus 0) \cdot 1 = 0$	$(0 \cdot 1) \oplus (0 \cdot 1) = 0$
0	1	0	$(0 \oplus 1) \cdot 0 = 0$	$(0 \cdot 0) \oplus (1 \cdot 0) = 0$
0	1	1	$(0 \oplus 1) \cdot 1 = 1$	$(0 \cdot 1) \oplus (1 \cdot 1) = 1$
1	0	0	$(1 \oplus 0) \cdot 0 = 0$	$(1 \cdot 0) \oplus (0 \cdot 0) = 0$
1	0	1	$(1 \oplus 0) \cdot 1 = 1$	$(1 \cdot 1) \oplus (0 \cdot 1) = 1$
1	1	0	$(1 \oplus 1) \cdot 0 = 0$	$(1 \cdot 0) \oplus (1 \cdot 0) = 0$
1	1	1	$(1 \oplus 1) \cdot 1 = 0$	$(1 \cdot 1) \oplus (1 \cdot 1) = 0$

Como los resultados de las dos últimas columnas de la tabla coinciden, queda probado que $(a \oplus b) \cdot c = (a \cdot c) \oplus (b \cdot c) \quad \forall a, b, c \in \{0, 1\}$.

2) Se analizarán los siguientes casos:

a) p par y q par

b) p impar y q impar

c) p par y q impar

d) p impar y q par

Entonces

a) Si p es par y q par $\Rightarrow p = 2k \wedge q = 2k'$ con $k, k' \in \mathbb{Z} \Rightarrow p + q = 2(k + k') \Rightarrow$

$\Rightarrow p + q$ es par $\Rightarrow$ el resto de dividir $(p + q)$ por 2 es 0 $\Rightarrow (p \oplus q) = 0$. Por lo tanto

$$(-1)^{p \oplus q} = (-1)^0 = 1$$

Por otro lado

$$(-1)^p \cdot (-1)^q = (-1)^{2k} \cdot (-1)^{2k'} = 1$$

En consecuencia, $(-1)^{p \oplus q} = (-1)^p \cdot (-1)^q$

b) Es similar al caso a).

c) Si p es par y q impar $\Rightarrow p = 2k \wedge q = 2k' + 1$ con $k, k' \in \mathbb{Z} \Rightarrow p + q = 2(k + k') + 1 \Rightarrow p + q$ es impar $\Rightarrow$ el resto de dividir $(p + q)$ por 2 es 1 $\Rightarrow (p \oplus q) = 1$. Por lo tanto

$$(-1)^{p \oplus q} = (-1)^1 = -1$$

Por otro lado

$$(-1)^p \cdot (-1)^q = (-1)^{2k} \cdot (-1)^{2k' + 1} = (-1)^{2k} \cdot (-1)^{2k'} \cdot (-1) = -1$$

En consecuencia, $(-1)^{p \oplus q} = (-1)^p \cdot (-1)^q$

d) Es similar al caso c).

3) Aplicando la definición de producto interno canónico se obtiene

$$\begin{aligned} z \cdot (x \oplus y) &= (z_1, z_2, \dots, z_n) \cdot (x_1 \oplus y_1, x_2 \oplus y_2, \dots, x_n \oplus y_n) = \\ &= z_1(x_1 \oplus y_1) + z_2(x_2 \oplus y_2) + \dots + z_n(x_n \oplus y_n) \end{aligned}$$

Utilizando los resultados de los incisos 1) y 2) resulta

$$\begin{aligned} (-1)^{z \cdot (x \oplus y)} &= (-1)^{z_1(x_1 \oplus y_1) + z_2(x_2 \oplus y_2) + \dots + z_n(x_n \oplus y_n)} = \\ &= (-1)^{z_1(x_1 \oplus y_1)} \cdot (-1)^{z_2(x_2 \oplus y_2)} \cdot \dots \cdot (-1)^{z_n(x_n \oplus y_n)} = \\ &= (-1)^{(z_1 x_1) \oplus (z_1 y_1)} \cdot (-1)^{(z_2 x_2) \oplus (z_2 y_2)} \cdot \dots \cdot (-1)^{(z_n x_n) \oplus (z_n y_n)} = \\ &= (-1)^{(z_1 x_1)} \cdot (-1)^{(z_1 y_1)} \cdot (-1)^{(z_2 x_2)} \cdot (-1)^{(z_2 y_2)} \cdot \dots \cdot (-1)^{(z_n x_n)} \cdot (-1)^{(z_n y_n)} = \\ &= (-1)^{(z_1 x_1)} \cdot (-1)^{(z_2 x_2)} \cdot (-1)^{(z_n x_n)} \cdot (-1)^{(z_1 y_1)} \cdot (-1)^{(z_2 y_2)} \cdot \dots \cdot (-1)^{(z_n y_n)} = \\ &= (-1)^{(z_1 x_1)} \cdot (-1)^{(z_2 x_2)} \cdot (-1)^{(z_n x_n)} \cdot (-1)^{(z_1 y_1)} \cdot (-1)^{(z_2 y_2)} \cdot \dots \cdot (-1)^{(z_n y_n)} = \\ &= (-1)^{(z_1 x_1) + (z_2 x_2) + \dots + (z_n x_n)} \cdot (-1)^{(z_1 y_1) + (z_2 y_2) + \dots + (z_n y_n)} = (-1)^{z \cdot x} \cdot (-1)^{z \cdot y} \end{aligned}$$

En consecuencia,

$$(-1)^{z \cdot (x \oplus y)} = (-1)^{z \cdot x} \cdot (-1)^{z \cdot y} \quad \blacksquare$$

La siguiente definición es una extensión de la definición de compuerta f , para una función booleana más general.

Definición 4.10: La compuerta f para una función booleana $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$

Dada una función booleana $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$, la compuerta f es una compuerta de $2n$ qubits definida por

$$U_f |x_1, x_2, \dots, x_n\rangle \otimes |y_1, y_2, \dots, y_n\rangle = |x_1, x_2, \dots, x_n\rangle \otimes |(y_1, y_2, \dots, y_n) \oplus f(x_1, x_2, \dots, x_n)\rangle$$

O expresado en forma simplificada

$$U_f |x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

Con $x = x_1, x_2, \dots, x_n \wedge y = y_1, y_2, \dots, y_n$

A continuación se introducirá el concepto de función booleana periódica. Su definición difiere ligeramente del de una función de variable real periódica, y es la siguiente:

Definición 4.11: Función booleana periódica

Una función booleana $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ es periódica si existe un vector booleano no nulo $T = (T_1, T_2, \dots, T_n)$ tal que verifica

$$f(x) = f(y) \Leftrightarrow y = x \vee y = x \oplus T$$

Con $x = (x_1, x_2, \dots, x_n)$, $y = (y_1, y_2, \dots, y_n) \in \{0, 1\}^n$

Observación 4.12

De la definición anterior resulta que si f es una función booleana periódica, de período T , y $x_0 \in \{0, 1\}^n$ entonces

$$\left\{ x \in \{0, 1\}^n / f(x) = f(x_0) \right\} = \{ x_0, x_0 \oplus T \}$$

Este resultado será tenido en cuenta cuando se analice el Algoritmo de Simon.

Ejemplo 4.13

Dada la función booleana $f : \{0, 1\}^3 \rightarrow \{0, 1\}^3$ definida por $f(x_1, x_2, x_3) = (x_1, x_2, 1)$. Probar que f es periódica.

Solución

Sea $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$ con $x \neq y$. Se verá que existe un vector booleano $T = (T_1, T_2, T_3)$ tal que

$$f(x) = f(y) \Leftrightarrow y = x \oplus T.$$

Como $f(x) = f(y)$ entonces $(x_1, x_2, 1) = (y_1, y_2, 1)$. De aquí resulta el sistema

$$\begin{cases} x_1 = y_1 \\ x_2 = y_2 \end{cases} \quad [1]$$

Por otro lado, como $y = x \oplus T$ entonces $(y_1, y_2, y_3) = (x_1 \oplus T_1, x_2 \oplus T_2, x_3 \oplus T_3)$
 Luego

$$\begin{cases} y_1 = x_1 \oplus T_1 \\ y_2 = x_2 \oplus T_2 \\ y_3 = x_3 \oplus T_3 \end{cases} \quad [2]$$

Reemplazando [1] en [2] se obtiene

$$\begin{cases} x_1 = x_1 \oplus T_1 \\ x_2 = x_2 \oplus T_2 \\ y_3 = x_3 \oplus T_3 \end{cases} \quad [3]$$

De la primera ecuación de [3] resulta que

$$T_1 = 0$$

Pues si $T_1 = 1$ entonces $x_1 = x_1 \oplus 1 \Rightarrow x_1 = \overline{x_1}$, lo cual es un absurdo.

De manera similar, de la segunda ecuación de [3] se obtiene que

$$T_2 = 0$$

Finalmente, de la tercera ecuación de [3] resulta que

$$T_3 = 1$$

Pues si $T_3 = 0 \Rightarrow y_3 = x_3 \Rightarrow (y_1, y_2, y_3) = (x_1, x_2, x_3)$, lo cual es una contradicción pues $x \neq y$. En consecuencia, f es periódica de período $T = (0, 0, 1)$.

En base a los conceptos y propiedades previamente definidos, se procederá a describir Algoritmo de Simon.

Algoritmo de Simon

Como se mencionó anteriormente, este algoritmo consiste en hallar el período $T = (T_0, T_1, \dots, T_{n-1})$ de una función booleana periódica $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$. Tiene la característica de que es preciso ejecutar más de una vez el circuito cuántico que implementa el algoritmo.

Dicho circuito posee $2n$ entradas: $q_1 = q_2 = \dots = q_n = q_{n+1} = \dots = q_{2n} = |0\rangle$. Los primeros n qubits forman el primer registro, mientras que los últimos n qubits constituyen el segundo registro del circuito. Su representación gráfica es la siguiente:

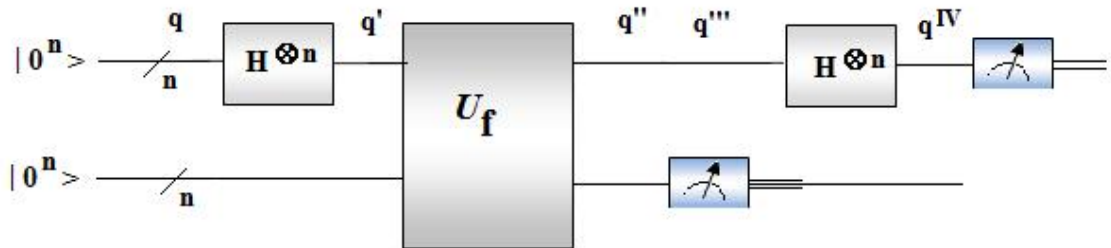


Figura 4.4: Circuito cuántico del algoritmo de Simon.

En este caso, el estado inicial del sistema es

$$q = q_1 \otimes q_2 \otimes \dots \otimes q_n \otimes \dots \otimes q_{2n} = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \dots \otimes |0\rangle = |0^n\rangle \otimes |0^n\rangle$$

Aplicando la Proposición 3.11, el siguiente estado del sistema es:

$$q' = H^{\otimes n} |0^n\rangle \otimes |0^n\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{0 \cdot x} |x\rangle \right) \otimes |0^n\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes |0^n\rangle \right)$$

Es decir,

$$q' = \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes |0^n\rangle \right)$$

Al atravesar la compuerta f el sistema evoluciona al siguiente estado:

$$\begin{aligned} q'' &= U_f q' = U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0^n\rangle \right) = \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} U_f (|x\rangle \otimes |0^n\rangle) \right) = \\ &= \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes |0^n \oplus f(x)\rangle \right) = \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle \right) = \sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}} |x\rangle \otimes |f(x)\rangle \end{aligned}$$

Luego

$$q'' = \sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}} |x\rangle \otimes \underbrace{|f(x)\rangle}_{\text{Segundo registro.}}$$

Ahora se efectúa la medición del segundo registro, es decir, de los n últimos qubits. En este caso, se obtendrá un n -qubit $|f(x_0)\rangle$, para algún $x_0 \in \{0, 1, \dots, 2^n - 1\}$ (el n -qubit $|x_0\rangle$ está expresado en base 10). Luego, por la Proposición 2.26, y teniendo en cuenta que

$$\{x / f(x) = f(x_0)\} = \{x_0, x_0 \oplus T\}$$

Entonces el sistema colapsa al siguiente estado:

$$\begin{aligned} q''' &= \frac{\left(\frac{1}{\sqrt{2^n}} |x_0\rangle + \frac{1}{\sqrt{2^n}} |x_0 \oplus T\rangle \right) \otimes |f(x_0)\rangle}{\sqrt{\left(\frac{1}{\sqrt{2^n}} \right)^2 + \left(\frac{1}{\sqrt{2^n}} \right)^2}} = \frac{\left(\frac{1}{\sqrt{2^n}} |x_0\rangle + \frac{1}{\sqrt{2^n}} |x_0 \oplus T\rangle \right) \otimes |f(x_0)\rangle}{\sqrt{\frac{1}{2^{n-1}}}} = \\ &= \frac{\left(\frac{1}{\sqrt{2^n}} |x_0\rangle + \frac{1}{\sqrt{2^n}} |x_0 \oplus T\rangle \right) \otimes |f(x_0)\rangle}{\sqrt{\frac{1}{2^{n-1}}}} = \frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus T\rangle) \otimes |f(x_0)\rangle \end{aligned}$$

Por lo tanto

$$q''' = \underbrace{\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus T\rangle)}_{\text{Primer registro}} \otimes |f(x_0)\rangle$$

Al aplicar la compuerta de Hadamard al primer registro, y teniendo en cuenta la Proposición 4.9 inciso 3), se obtiene

$$\begin{aligned} q^{IV} &= H^{\otimes n} \left(\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus T\rangle) \right) \otimes |f(x_0)\rangle = \frac{1}{\sqrt{2}} (H^{\otimes n} |x_0\rangle + H^{\otimes n} |x_0 \oplus T\rangle) \otimes |f(x_0)\rangle = \\ &= \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y} |y\rangle + \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{(x_0 \oplus T) \cdot y} |y\rangle \right) \otimes |f(x_0)\rangle = \\ &= \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} \left((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus T) \cdot y} \right) |y\rangle \right) \otimes |f(x_0)\rangle = \\ &= \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} \left((-1)^{x_0 \cdot y} + (-1)^{x_0 \cdot y} (-1)^{T \cdot y} \right) |y\rangle \right) \otimes |f(x_0)\rangle = \\ &= \left(\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y} \left(1 + (-1)^{T \cdot y} \right) |y\rangle \right) \otimes |f(x_0)\rangle = \\ &= \left(\sum_{y=0}^{2^n-1} \frac{1}{\sqrt{2^{n+1}}} (-1)^{x_0 \cdot y} \left(1 + (-1)^{T \cdot y} \right) |y\rangle \right) \otimes |f(x_0)\rangle \end{aligned}$$

Luego

$$q^{IV} = \underbrace{\left(\sum_{y=0}^{2^n-1} \frac{1}{\sqrt{2^{n+1}}} (-1)^{x_0 \cdot y} \left(1 + (-1)^{T \cdot y} \right) |y\rangle \right)}_{\text{Primer registro}} \otimes |f(x_0)\rangle$$

Finalmente se mide el primer registro. Si se define, para $i = 0, 1, \dots, 2^n - 1$:

$P(y_i)$ = Probabilidad de que el primer registro, al ser observado, esté en el estado $|y_i\rangle$.

Entonces, por la Proposición 2.9, se tiene

$$P(y_i) = \left| \frac{1}{\sqrt{2^{n+1}}} (-1)^{x_0 \cdot y_i} \left(1 + (-1)^{T \cdot y_i} \right) \right|^2 =$$

$$= \begin{cases} \left| \frac{1}{\sqrt{2^{n+1}}} (-1)^{x_0 \cdot y_i} (1+1) \right|^2 & \text{si } T \cdot y_i \text{ es par} \\ \left| \frac{1}{\sqrt{2^{n+1}}} (-1)^{x_0 \cdot y_i} (1-1) \right|^2 & \text{si } T \cdot y_i \text{ es impar} \end{cases} = \begin{cases} \left| \frac{1}{\sqrt{2^{n+1}}} (-1)^{x_0 \cdot y_i} (2) \right|^2 & \text{si } T \cdot y_i \text{ es par} \\ \left| \frac{1}{\sqrt{2^{n+1}}} (-1)^{x_0 \cdot y_i} (0) \right|^2 & \text{si } T \cdot y_i \text{ es impar} \end{cases}$$

$$= \begin{cases} \frac{1}{2^{n-1}} & \text{si } T \cdot y_i \text{ es par} \\ 0 & \text{si } T \cdot y_i \text{ es impar} \end{cases} = \begin{cases} \frac{1}{2^{n-1}} & \text{si } T \cdot y_i \equiv 0 \pmod{2} \\ 0 & \text{si } T \cdot y_i \equiv 1 \pmod{2} \end{cases}$$

En consecuencia

$$P(y_i) = \begin{cases} \frac{1}{2^{n-1}} & \text{si } T \cdot y_i \equiv 0 \pmod{2} \\ 0 & \text{si } T \cdot y_i \equiv 1 \pmod{2} \end{cases}$$

Este resultado probabilístico indica que, al ejecutar el algoritmo y efectuar la medición del primer registro, se obtiene un n-qubit $|y_i\rangle$ que verifica la ecuación

$$T.y_i \equiv 0 \pmod{2}$$

Pues el caso en que $T.y_i \equiv 1 \pmod{2}$ tiene probabilidad nula de ocurrir.

El análisis anteriormente expuesto permite elaborar la siguiente:

Conclusión

Para hallar el período $T = (T_0, T_1, \dots, T_{n-1})$ de una función booleana periódica $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ se procede así:

1) Se ejecuta el circuito cuántico de Simon tantas veces hasta obtener las mediciones $|y_i\rangle = |y_{i,n-1} \ y_{i,n-2} \ \dots y_{i,1} \ y_{i,0}\rangle$, con $i = 1, 2, \dots, n-1$, de modo tal que los vectores $\overrightarrow{y_i} = (y_{i,0}, y_{i,1}, \dots, y_{i,n-2}, y_{i,n-1})$ sean linealmente independientes $\forall \ i = 1, 2, \dots, n-1$.

2) Se resuelve el sistema lineal

$$\begin{cases} T.y_1 \equiv 0 \pmod{2} \\ T.y_2 \equiv 0 \pmod{2} \\ \dots\dots\dots \\ T.y_{n-1} \equiv 0 \pmod{2} \end{cases}$$

Donde $T.y_i = T_0.y_{i,0} + T_1.y_{i,1} + \dots + T_{n-1}.y_{i,n-1}$, $\forall i = 1, 2, \dots, n-1$.

Se puede probar que dicho sistema tendrá una única solución no trivial (véase [10]), que darán las componentes del período T .

Ejemplo 4.14

Se desea hallar el período $T = (T_0, T_1, T_2, T_3)$ de una función booleana $f : \{0, 1\}^4 \rightarrow \{0, 1\}^4$.

1) Se ejecutó tres veces el circuito de Simon y se obtuvieron los 4-qubits:

$$|y_1\rangle = |0100\rangle, |y_2\rangle = |1000\rangle, |y_3\rangle = |1100\rangle$$

¿Se puede resolver el sistema

$$\begin{cases} T \cdot y_1 \equiv 0 \pmod{2} \\ T \cdot y_2 \equiv 0 \pmod{2} \\ T \cdot y_3 \equiv 0 \pmod{2} \end{cases}$$

Para hallar la única solución no nula T ?

2) Si al correr tres veces el circuito de Simon se hubieran obtenido los 4-qubits:

$$|y_1\rangle = |0011\rangle, |y_2\rangle = |1010\rangle, |y_3\rangle = |0101\rangle$$

¿Se puede hallar el período T ?

Solución

1) Como los vectores $\vec{y}_1 = (0, 0, 1, 0)$, $\vec{y}_2 = (0, 0, 0, 1)$, $\vec{y}_3 = (0, 0, 1, 1)$ no son linealmente independientes, el sistema no puede generar una única solución no nula T .

2) Como los vectores $\vec{y}_1 = (1, 1, 0, 0)$, $\vec{y}_2 = (0, 1, 0, 1)$, $\vec{y}_3 = (1, 0, 1, 0)$ son linealmente independientes, el sistema tendrá única solución no nula. Se resuelve entonces el sistema

$$\begin{cases} T \cdot y_1 \equiv 0 \pmod{2} \\ T \cdot y_2 \equiv 0 \pmod{2} \\ T \cdot y_3 \equiv 0 \pmod{2} \end{cases} \Rightarrow \begin{cases} T_0 \cdot 1 + T_1 \cdot 1 + T_2 \cdot 0 + T_3 \cdot 0 \equiv 0 \pmod{2} \\ T_0 \cdot 0 + T_1 \cdot 1 + T_2 \cdot 0 + T_3 \cdot 1 \equiv 0 \pmod{2} \\ T_0 \cdot 1 + T_1 \cdot 0 + T_2 \cdot 1 + T_3 \cdot 0 \equiv 0 \pmod{2} \end{cases}$$

Para hallar la solución de este sistema se aplica el Método de Sustitución o bien el Método de Eliminación de Gauss. A modo de ejemplo se utilizará este último, teniendo en cuenta que $-1 \equiv 0 \pmod{2}$:

$$\begin{aligned} \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{array} \right) &\rightarrow \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 & 0 \end{array} \right) \equiv \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{array} \right) \rightarrow \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \end{array} \right) \equiv \\ &\equiv \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array} \right) \end{aligned}$$

Por lo tanto, se resuelve el sistema

$$\begin{cases} T_2 + T_3 \equiv 0 \pmod{2} & [1] \\ T_1 + T_3 \equiv 0 \pmod{2} & [2] \\ T_0 + T_1 \equiv 0 \pmod{2} & [3] \end{cases}$$

De la ecuación [1] resulta que $(T_2 = T_3 = 0) \vee (T_2 = T_3 = 1)$.

Primer Caso: $T_2 = T_3 = 0$

De la ecuación [2] se tiene

$$T_1 + T_3 \equiv 0 \pmod{2} \Rightarrow T_1 + 0 \equiv 0 \pmod{2} \Rightarrow T_1 \equiv 0 \pmod{2} \Rightarrow T_1 = 0$$

De manera similar, de la ecuación [3] resulta que $T_0 = 0$. En consecuencia,

$T = (0, 0, 0, 0)$ es solución del sistema.

Segundo Caso: $T_2 = T_3 = 1$

De la ecuación [2] se tiene

$$T_1 + T_3 \equiv 0 \pmod{2} \Rightarrow T_1 + 1 \equiv 0 \pmod{2} \Rightarrow T_1 \equiv -1 \pmod{2} \Rightarrow T_1 \equiv 1 \pmod{2} \Rightarrow T_1 = 1$$

De manera similar, de la ecuación [3] resulta que $T_0 = 1$. En consecuencia,

$T = (1, 1, 1, 1)$ es solución del sistema.

Luego, el conjunto solución es $\{(0, 0, 0, 0), (1, 1, 1, 1)\}$. Como el período es un vector booleano no nulo, se deduce que el período de la función booleana es $T = (1, 1, 1, 1)$.

Observación 4.14

El Algoritmo de Simon combina la computación cuántica con la clásica, ya que para resolver el sistema $T \cdot y_i \equiv 0 \pmod{2}$, $i=1, 2, \dots, n-1$ se recurre a un ordenador convencional.

Por otro lado, en un algoritmo clásico, como el período de una función booleana

$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ es un vector no nulo de n componentes, en el peor de los casos

habría que evaluar f sobre $2^n - 1$ posibles vectores candidatos para ser el período T .

En cambio, en el Algoritmo de Simon, para obtener T se requiere repetir el circuito $O(n)$ veces que evaluar f . Por esta razón se dice que el Algoritmo de Simon es exponencialmente más eficiente que cualquier algoritmo clásico.

Capítulo 5

La Transformada Cuántica de Fourier

Como se sabe, la Computación Cuántica opera con compuertas que matemáticamente se describen mediante transformaciones lineales unitarias. En este capítulo se analizará una transformación unitaria muy importante, que será el corazón del Algoritmo de Shor: *La Transformada Cuántica de Fourier* (En inglés **Quantum Fourier Transform**). Su definición se basa en la *Transformada Discreta de Fourier*, como se verá a continuación.

Definición 5.1: Transformada Discreta de Fourier

Sea $p \in \mathbb{N}$ y $f : \mathbb{Z}_p \rightarrow \mathbb{C}$. La Transformada Discreta de Fourier de f es una función

$\tilde{f} : \mathbb{Z}_p \rightarrow \mathbb{C}$ definida por

$$\tilde{f}(x) = \frac{1}{\sqrt{p}} \sum_{y=0}^{p-1} f(y) e^{\frac{2\pi i x \cdot y}{p}}$$

Con $x \in \mathbb{Z}_p = \{0, 1, \dots, p-1\}$

Ejemplo 5.2

Sea $f : \mathbb{Z}_2 \rightarrow \mathbb{C}$ definida por

$$\begin{cases} f(0) = 1 \\ f(1) = 2 \end{cases}$$

Calcular la Transformada Discreta de Fourier de f .

Solución

En este caso, $p = 2$. Luego

$$\tilde{f}(x) = \frac{1}{\sqrt{p}} \sum_{y=0}^{p-1} f(y) e^{\frac{2\pi i x \cdot y}{p}} = \frac{1}{\sqrt{2}} \sum_{y=0}^{2-1} f(y) e^{\frac{2\pi i x \cdot y}{2}} = \frac{1}{\sqrt{2}} \sum_{y=0}^1 f(y) e^{\pi i x \cdot y}$$

Por lo tanto

$$\begin{aligned} \tilde{f}(0) &= \frac{1}{\sqrt{2}} \sum_{y=0}^1 f(y) e^{\pi i 0 \cdot y} = \frac{1}{\sqrt{2}} \sum_{y=0}^1 f(y) \cdot 1 = \frac{1}{\sqrt{2}} (f(0) + f(1)) = \frac{1}{\sqrt{2}} (1 + 2) = \\ &= \frac{3}{\sqrt{2}} \end{aligned}$$

$$\tilde{f}(1) = \frac{1}{\sqrt{2}} \sum_{y=0}^1 f(y) e^{\pi i 1 \cdot y} = \frac{1}{\sqrt{2}} \sum_{y=0}^1 f(y) \cdot e^{\pi i y} = \frac{1}{\sqrt{2}} (f(0)e^{\pi i \cdot 0} + f(1)e^{\pi i \cdot 1}) =$$

$$= \frac{1}{\sqrt{2}} (f(0) \cdot 1 + f(1)(-1)) = \frac{1}{\sqrt{2}} (1 - 2) = -\frac{1}{\sqrt{2}}$$

Para definir la Transformada Cuántica de Fourier sobre el espacio de los n -qubits, basta definirla para los elementos de una base de dicho espacio. Como se sabe, una base es:

$$\{ |x_{n-1} x_{n-2} \dots x_1 x_0\rangle \text{ con } x_i = 0 \text{ ó } 1, i = 0, 1, \dots, n-1 \}$$

Por otro lado, en el Capítulo 2 se vio que, para simplificar la notación, se utiliza la siguiente identificación de los qubits de dicha base:

$$|x_{n-1} x_{n-2} \dots x_1 x_0\rangle \equiv |x\rangle$$

Donde x es la representación en base 10 del número binario $x_{n-1} x_{n-2} \dots x_1 x_0$.

Como

$$|x_{n-1} x_{n-2} \dots x_1 x_0\rangle \equiv |x\rangle \in \{ |0\rangle, |1\rangle, |2\rangle, \dots, |2^n - 1\rangle \}$$

A los elementos de esta base se los puede asociar con elementos de $\mathbb{Z}_{2^n}$. Este hecho sugiere definir la Transformada Cuántica de Fourier de manera similar a la Definición 5.1 considerando $p = 2^n$, como se indica a continuación:

Definición 5.3: La Transformada Cuántica de Fourier de n -qubits

Sea $|x\rangle \in \{ |0\rangle, |1\rangle, |2\rangle, \dots, |2^n - 1\rangle \}$ un elemento de la base del espacio de los n -qubits. La Transformada Cuántica de Fourier, simbolizada mediante la sigla QFT, es la transformación lineal definida por

$$QFT |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} |y\rangle e^{\frac{2\pi i x \cdot y}{2^n}}$$

Donde

$|x\rangle$ es la representación en base 10 del n -qubit $|x_{n-1} x_{n-2} \dots x_1 x_0\rangle$

$|y\rangle$ es la representación en base 10 del n -qubit $|y_{n-1} y_{n-2} \dots y_1 y_0\rangle$

Se puede comprobar que si $n = 1$, la Transformada Cuántica de Fourier es la compuerta de Hadamard. El siguiente Ejemplo ilustra cómo calcular dicha Transformada.

Ejemplo 5.4

Sea $n=3$. Calcular $QFT |5\rangle$.

Solución

$$QFT |5\rangle = \frac{1}{\sqrt{2^3}} \sum_{y=0}^{2^3-1} |y\rangle e^{\frac{2\pi i x \cdot y}{2^3}} = \frac{1}{\sqrt{2^3}} \sum_{y=0}^7 |y\rangle e^{\frac{\pi i x \cdot y}{4}} =$$

$$\begin{aligned}
&= \frac{1}{\sqrt{2^3}} \left(|0\rangle e^{\frac{\pi i 5 \cdot (0)}{4}} + |1\rangle e^{\frac{\pi i 5 \cdot (1)}{4}} + |2\rangle e^{\frac{\pi i 5 \cdot (2)}{4}} + |3\rangle e^{\frac{\pi i 5 \cdot (3)}{4}} + |4\rangle e^{\frac{\pi i 5 \cdot (4)}{4}} + \right. \\
&\quad \left. + |5\rangle e^{\frac{\pi i 5 \cdot (5)}{4}} + |6\rangle e^{\frac{\pi i 5 \cdot (6)}{4}} + |7\rangle e^{\frac{\pi i 5 \cdot (7)}{4}} \right) = \\
&= \frac{1}{\sqrt{2^3}} \left(|0\rangle + |1\rangle e^{\frac{\pi i 5}{4}} + |2\rangle e^{\frac{\pi i 5}{2}} + |3\rangle e^{\frac{\pi i 15}{4}} + |4\rangle e^{\pi i 5} + \right. \\
&\quad \left. + |5\rangle e^{\frac{\pi i 25}{4}} + |6\rangle e^{\frac{\pi i 30}{4}} + |7\rangle e^{\frac{\pi i 35}{4}} \right)
\end{aligned}$$

Por lo tanto

$$QFT |5\rangle = \frac{1}{\sqrt{2^3}} \left(|0\rangle + |1\rangle e^{\frac{5}{4}\pi i} + |2\rangle i + |3\rangle e^{\frac{15}{4}\pi i} - |4\rangle + |5\rangle e^{\frac{\pi i 25}{4}} - |6\rangle i + |7\rangle e^{\frac{\pi i 35}{4}} \right)$$

O equivalentemente

$$\begin{aligned}
QFT |101\rangle &= \frac{1}{\sqrt{2^3}} \left(|000\rangle + |001\rangle e^{\frac{5}{4}\pi i} + |010\rangle i + |011\rangle e^{\frac{15}{4}\pi i} - |100\rangle + |101\rangle e^{\frac{\pi i 25}{4}} + \right. \\
&\quad \left. - |110\rangle i + |111\rangle e^{\frac{\pi i 35}{4}} \right)
\end{aligned}$$

Representación matricial de la Transformada Cuántica de Fourier

La Transformada Cuántica de Fourier, por ser una transformación lineal, tiene una representación matricial. Para hallarla, se valorará la Transformada en cada uno de los elementos de la siguiente base del espacio de los n-qubits expresados, para simplificar la escritura, en representación decimal:

$$\{ |0\rangle, |1\rangle, |2\rangle, \dots, |2^n - 1\rangle \}$$

Entonces, si se define $w = e^{\frac{2\pi i}{2^n}}$ se obtiene

$$QFT |0\rangle = \frac{1}{\sqrt{2^n}} \left(1 \cdot |0\rangle + 1 \cdot |1\rangle + 1 \cdot |2\rangle + \dots + 1 \cdot |2^n - 1\rangle \right)$$

$$QFT |1\rangle = \frac{1}{\sqrt{2^n}} \left(1 \cdot |0\rangle + w \cdot |1\rangle + w^2 \cdot |2\rangle + \dots + w^{2^n - 1} \cdot |2^n - 1\rangle \right)$$

$$QFT |2\rangle = \frac{1}{\sqrt{2^n}} \left(1 \cdot |0\rangle + w^2 \cdot |1\rangle + w^4 \cdot |2\rangle + \dots + w^{2(2^n - 1)} \cdot |2^n - 1\rangle \right)$$

.....

$$QFT \left| 2^n - 1 \right\rangle = \frac{1}{\sqrt{2^n}} \left(1 \cdot |0\rangle + w^{2^n-1} |1\rangle + w^{(2^n-1) \cdot 2} |2\rangle + \dots + w^{(2^n-1)(2^n-1)} |2^n-1\rangle \right)$$

Por lo tanto, la matriz asociada a la Transformada Cuántica de Fourier sobre el espacio de los n -qubits es:

$$F_n = \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & w^3 & \dots & w^{2^n-1} \\ 1 & w^2 & w^4 & w^6 & \dots & w^{2(2^n-1)} \\ 1 & w^3 & w^6 & w^9 & \dots & w^{3(2^n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{2^n-1} & w^{2(2^n-1)} & w^{3(2^n-1)} & \dots & w^{(2^n-1)(2^n-1)} \end{pmatrix}$$

Se puede comprobar fácilmente que F_n es efectivamente una matriz unitaria.

Diseño del circuito cuántico para la Transformada Cuántica de Fourier

La Transformada Cuántica de Fourier puede ser diseñada eficientemente en un ordenador cuántico, utilizando tres tipos de compuertas: *la compuerta de Hadamard*, *la compuerta de Desplazamiento de Fase* y *la compuerta Swap*.

En esta sección se verá cómo crear un circuito cuántico asociado a esta Transformada.

Se probará además que requerirá $O(n^2)$ compuertas cuánticas, donde n es el número de qubits. Previamente se recordarán algunas definiciones y se demostrarán propiedades que serán utilizadas en el armado de dicho circuito.

Compuertas que intervienen en el circuito de la transformada cuántica de Fourier

Como se mencionó anteriormente, las compuertas que se emplearán para el diseño del circuito son tres:

1- La compuerta de Hadamard para un qubit

Como se vio en el Capítulo 3, la matriz asociada a esta compuerta es:

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Como

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Entonces la compuerta de Hadamard puede expresarse del siguiente modo:

$$H|x\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i (0.x)} |1\rangle)$$

Donde

$$x \in \{0,1\}$$

$0.x$ es un número binario, cuya representación en base 10 es : $0.x = x \cdot 2^{-1}$.

De este modo,

$$e^{2\pi i (0.x)} = e^{2\pi i x 2^{-1}} = e^{\pi i x} = \cos(\pi x) + i \sin(\pi x) = \begin{cases} 1 & \text{si } x = 0 \\ -1 & \text{si } x = 1 \end{cases}$$

Esta nueva manera de expresar la compuerta de Hadamard será utilizada en el diseño del circuito de la Transformada Cuántica de Fourier.

2- La compuerta R_θ de Desplazamiento de Fase

Dado un ángulo θ expresado en radianes, la representación matricial de esta compuerta es:

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

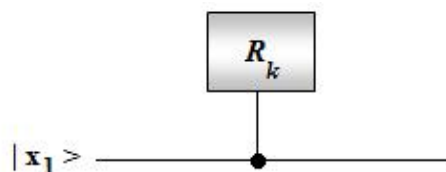
En particular, se define la siguiente compuerta, considerando $\theta = \frac{2\pi}{2^k}$:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$$

Dicha compuerta opera sobre un determinado bit. Por ejemplo, si R_k opera sobre el bit x_1 , entonces su expresión queda:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i x_1}{2^k}} \end{pmatrix}$$

Y su representación gráfica es:

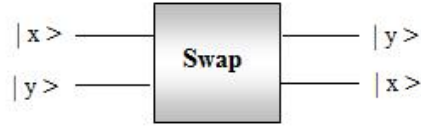


3- La compuerta Swap

Esta compuerta intercambia dos qubits y se la define por

$$\text{Swap } |x y\rangle = |y x\rangle \text{ con } x, y \in \{0, 1\}.$$

La representación gráfica es:



La siguiente Proposición se utilizará para demostrar otra forma de representación de la Transformada cuántica de Fourier.

Proposición 5.5

Si $x_i, y_i \in \{0, 1\} \forall i=1, 2, \dots, n$ entonces

$$\sum_{i=1}^n \sum_{j=1}^n (|x_i\rangle \otimes |y_j\rangle) = \left(\sum_{i=1}^n |x_i\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle \right)$$

Demostración

Se aplicará el principio de Inducción sobre n .

Para $n = 1$

Se verifica pues

$$\sum_{i=1}^1 \sum_{j=1}^1 (|x_i\rangle \otimes |y_j\rangle) = |x_1\rangle \otimes |y_1\rangle = \left(\sum_{i=1}^1 |x_i\rangle \right) \otimes \left(\sum_{j=1}^1 |y_j\rangle \right)$$

Se supone que la igualdad es válida para n (Hipótesis Inductiva).

Es decir,

$$\sum_{i=1}^n \sum_{j=1}^n (|x_i\rangle \otimes |y_j\rangle) = \left(\sum_{i=1}^n |x_i\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle \right)$$

Se probará que la afirmación es válida para $(n+1)$

O sea, se verificará que

$$\sum_{i=1}^{n+1} \sum_{j=1}^{n+1} (|x_i\rangle \otimes |y_j\rangle) = \left(\sum_{i=1}^{n+1} |x_i\rangle \right) \otimes \left(\sum_{j=1}^{n+1} |y_j\rangle \right)$$

Entonces

$$\begin{aligned}
& \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} (|x_i\rangle \otimes |y_j\rangle) = \sum_{i=1}^{n+1} \left(\sum_{j=1}^n (|x_i\rangle \otimes |y_j\rangle) + (|x_i\rangle \otimes |y_{n+1}\rangle) \right) = \\
& \sum_{i=1}^{n+1} \sum_{j=1}^n (|x_i\rangle \otimes |y_j\rangle) + \sum_{i=1}^{n+1} (|x_i\rangle \otimes |y_{n+1}\rangle) = \underbrace{\sum_{i=1}^n \sum_{j=1}^n (|x_i\rangle \otimes |y_j\rangle)}_{\text{Hipótesis Inductiva}} + \\
& + \sum_{j=1}^n (|x_{n+1}\rangle \otimes |y_j\rangle) + \sum_{i=1}^{n+1} (|x_i\rangle \otimes |y_{n+1}\rangle) = \\
& = \left(\sum_{i=1}^n |x_i\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle \right) + \sum_{j=1}^n (|x_{n+1}\rangle \otimes |y_j\rangle) + \sum_{i=1}^{n+1} (|x_i\rangle \otimes |y_{n+1}\rangle) = \\
& = \left(\sum_{i=1}^n |x_i\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle \right) + \sum_{j=1}^n (|x_{n+1}\rangle \otimes |y_j\rangle) + \sum_{i=1}^n (|x_i\rangle \otimes |y_{n+1}\rangle) + (|x_{n+1}\rangle \otimes |y_{n+1}\rangle)
\end{aligned}$$

Por lo tanto

$$\begin{aligned}
& \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} (|x_i\rangle \otimes |y_j\rangle) = \left(\sum_{i=1}^n |x_i\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle \right) + \sum_{j=1}^n (|x_{n+1}\rangle \otimes |y_j\rangle) + \\
& + \sum_{i=1}^n (|x_i\rangle \otimes |y_{n+1}\rangle) + (|x_{n+1}\rangle \otimes |y_{n+1}\rangle) \quad [1]
\end{aligned}$$

Por otro lado, por la Proposición 1.9, incisos 1) y 2) resulta

$$\begin{aligned}
& \left(\sum_{i=1}^{n+1} |x_i\rangle \right) \otimes \left(\sum_{j=1}^{n+1} |y_j\rangle \right) = \left(\sum_{i=1}^n |x_i\rangle + |x_{n+1}\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle + |y_{n+1}\rangle \right) = \\
& = \left(\sum_{i=1}^n |x_i\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle \right) + \left(\sum_{i=1}^n |x_i\rangle \right) \otimes |y_{n+1}\rangle + |x_{n+1}\rangle \otimes \left(\sum_{j=1}^n |y_j\rangle \right) + (|x_{n+1}\rangle \otimes |y_{n+1}\rangle) = \\
& = \left(\sum_{i=1}^n |x_i\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle \right) + \left(\sum_{i=1}^n |x_i\rangle \otimes |y_{n+1}\rangle \right) + \left(\sum_{j=1}^n |x_{n+1}\rangle \otimes |y_j\rangle \right) + (|x_{n+1}\rangle \otimes |y_{n+1}\rangle)
\end{aligned}$$

En consecuencia

$$\begin{aligned}
& \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} (|x_i\rangle \otimes |y_j\rangle) = \left(\sum_{i=1}^n |x_i\rangle \right) \otimes \left(\sum_{j=1}^n |y_j\rangle \right) + \left(\sum_{i=1}^n |x_i\rangle \otimes |y_{n+1}\rangle \right) + \\
& + \left(\sum_{j=1}^n |x_{n+1}\rangle \otimes |y_j\rangle \right) + (|x_{n+1}\rangle \otimes |y_{n+1}\rangle) \quad [2]
\end{aligned}$$

De [1] y [2] se deduce que $\sum_{i=1}^{n+1} \sum_{j=1}^{n+1} (|x_i\rangle \otimes |y_j\rangle) = \left(\sum_{i=1}^{n+1} |x_i\rangle \right) \otimes \left(\sum_{j=1}^{n+1} |y_j\rangle \right)$ ■

A continuación se probará otra forma de expresar la Transformada Cuántica de Fourier, que se utilizará para el diseño de su circuito cuántico.

Proposición 5.6

Si $x_i \in \{0, 1\} \forall i = 0, 1, \dots, n-1$ entonces

$$QFT |x_{n-1} \dots x_0\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \otimes \dots \otimes \left(|0\rangle + e^{2\pi i 0.x_{n-1} \dots x_0} |1\rangle \right)$$

Es decir

$$QFT |x_{n-1} x_{n-2} \dots x_1 x_0\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^n \left(|0\rangle + e^{2\pi i 0.x_{l-1} x_{l-2} \dots x_0} |1\rangle \right)$$

Donde

$$0.x_{l-1} x_{l-2} \dots x_1 x_0 = x_{l-1} \cdot 2^{-1} + x_{l-2} \cdot 2^{-2} + \dots + x_1 \cdot 2^{-(l-1)} + x_0 \cdot 2^{-(l-0)}$$

O equivalentemente

$$0.x_{l-1} x_{l-2} \dots x_1 x_0 = \sum_{k=1}^l x_{l-k} \cdot 2^{-k}$$

Demostración

De acuerdo a la definición de Transformada Cuántica de Fourier, se tiene

$$QFT |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} |y\rangle e^{\frac{2\pi i x \cdot y}{2^n}}$$

Donde

$|x\rangle$ es la representación en base 10 del n-qubit $|x_{n-1} x_{n-2} \dots x_1 x_0\rangle$

$|y\rangle$ es la representación en base 10 del n-qubit $|y_{n-1} y_{n-2} \dots y_1 y_0\rangle$

Por lo tanto, la expresión en base 10 del número y es

$$y = y_0 \cdot 2^0 + y_1 \cdot 2^1 + \dots + y_{n-1} \cdot 2^{n-1} = \sum_{k=0}^{n-1} y_k \cdot 2^k$$

Luego

$$\frac{2\pi i x \cdot y}{2^n} = \frac{2\pi i x}{2^n} \sum_{k=0}^{n-1} y_k \cdot 2^k = 2\pi i x \sum_{k=0}^{n-1} y_k \cdot 2^{k-n} = 2\pi i x \sum_{k=0}^{n-1} y_k \cdot \frac{1}{2^{n-k}} =$$

$$= 2\pi i x \underbrace{\sum_{l=n}^1 y_{n-l} \cdot \frac{1}{2^l}}_{\text{Se sustituye } l = n - k} = 2\pi i x \sum_{l=1}^n y_{n-l} \cdot \frac{1}{2^l}$$

Se sustituye $l = n - k$

Es decir

$$\frac{2\pi i x y}{2^n} = 2\pi i x \sum_{l=1}^n y_{n-l} \cdot \frac{1}{2^l}$$

Reemplazando esta expresión en la Transformada Cuántica de Fourier se obtiene

$$QFT |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y_{n-1}=0}^1 \sum_{y_{n-2}=0}^1 \dots \sum_{y_0=0}^1 e^{i \sum_{l=1}^n \frac{2\pi x}{2^l} y_{n-l}} |y_{n-1} y_{n-2} \dots y_1 y_0\rangle$$

Aplicando la Proposición 5.5, la propiedad de que la exponencial de una suma es el producto de las exponenciales y que

$$|y_{n-1} y_{n-2} \dots y_1 y_0\rangle = |y_{n-1}\rangle \otimes |y_{n-2}\rangle \otimes \dots \otimes |y_1\rangle \otimes |y_0\rangle$$

Entonces

$$\begin{aligned} QFT |x\rangle &= \frac{1}{\sqrt{2^n}} \sum_{y_{n-1}=0}^1 \sum_{y_{n-2}=0}^1 \dots \sum_{y_0=0}^1 e^{i \sum_{l=1}^n \frac{2\pi x}{2^l} y_{n-l}} |y_{n-1}\rangle \otimes |y_{n-2}\rangle \otimes \dots \otimes |y_1\rangle \otimes |y_0\rangle = \\ &= \frac{1}{\sqrt{2^n}} \sum_{y_{n-1}=0}^1 e^{i \frac{2\pi x}{2^1} y_{n-1}} \sum_{y_{n-2}=0}^1 e^{i \frac{2\pi x}{2^2} y_{n-2}} \dots \sum_{y_0=0}^1 e^{i \frac{2\pi x}{2^n} y_0} |y_{n-1}\rangle \otimes |y_{n-2}\rangle \otimes \dots \otimes |y_1\rangle \otimes |y_0\rangle = \\ &= \frac{1}{\sqrt{2^n}} \left[\sum_{y_{n-1}=0}^1 e^{i \frac{2\pi x}{2^1} y_{n-1}} |y_{n-1}\rangle \otimes \sum_{y_{n-2}=0}^1 e^{i \frac{2\pi x}{2^2} y_{n-2}} |y_{n-2}\rangle \otimes \dots \otimes \sum_{y_0=0}^1 e^{i \frac{2\pi x}{2^n} y_0} |y_0\rangle \right] = \\ &= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^n \left[|0\rangle + e^{i \frac{2\pi x}{2^l}} |1\rangle \right] \end{aligned}$$

Por lo tanto

$$QFT |x\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^n \left[|0\rangle + e^{i \frac{2\pi x}{2^l}} |1\rangle \right] \quad [1]$$

Por otro lado, la expresión en base 10 del número x es

$$x = x_0 \cdot 2^0 + x_1 \cdot 2^1 + \dots + x_{n-1} \cdot 2^{n-1} = \sum_{k=0}^{n-1} x_k \cdot 2^k$$

Luego

$$\frac{x}{2^l} = \sum_{k=0}^{n-1} x_k \cdot 2^{k-l} = \sum_{k=0}^{l-1} x_k \cdot 2^{k-l} + \sum_{k=l}^{n-1} x_k \cdot 2^{k-l}$$

Teniendo en cuenta que $\sum_{k=l}^{n-1} x_k \cdot 2^{k-l}$ es un número natural y que $e^{2\pi i n} = 1 \quad \forall n \in \mathbb{N}$ resulta

$$\begin{aligned} e^{\frac{2\pi i x}{2^l}} &= e^{2\pi i \left(\sum_{k=0}^{l-1} x_k \cdot 2^{k-l} + \sum_{k=l}^{n-1} x_k \cdot 2^{k-l} \right)} = e^{2\pi i \left(\sum_{k=0}^{l-1} x_k \cdot 2^{k-l} \right)} \cdot \underbrace{e^{2\pi i \left(\sum_{k=l}^{n-1} x_k \cdot 2^{k-l} \right)}}_{=1} = \\ &= e^{2\pi i \left(\sum_{k=0}^{l-1} x_k \cdot 2^{k-l} \right)} = e^{2\pi i \cdot 0.x_{l-1} x_{l-2} \dots x_1 x_0} \end{aligned}$$

Luego

$$e^{\frac{2\pi i x}{2^l}} = e^{2\pi i \cdot 0.x_{l-1} x_{l-2} \dots x_1 x_0} \quad [2]$$

Sustituyendo [2] en [1] resulta finalmente

$$QFT |x_{n-1} x_{n-2} \dots x_1 x_0\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^n \left(|0\rangle + e^{2\pi i \cdot 0.x_{l-1} x_{l-2} \dots x_0} |1\rangle \right) \quad \blacksquare$$

Circuito cuántico para la Transformada Cuántica de Fourier

En la Proposición 5.6 se demostró que la Transformada Cuántica de Fourier puede ser “factorizada” como producto tensorial de n qubits. Este resultado permitirá diseñar el circuito cuántico asociado a dicha Transformada de una manera sencilla, empleando solamente compuertas de Hadamard, de Desplazamiento de Fase y compuertas Swaps.

Por cuestiones didácticas se mostrará cómo crear dicho circuito para un qubit, luego para dos y tres qubits, para proceder finalmente a la generalización a n qubits.

Circuito Cuántico de la QFT de 1-qubit

En este caso, $n = 1$. Según la Proposición 5.6, se tiene que si $x_0 \in \{0, 1\}$ entonces

$$\begin{aligned} QFT |x_0\rangle &= \frac{1}{\sqrt{2^1}} \bigotimes_{l=1}^1 \left(|0\rangle + e^{2\pi i \cdot 0.x_{l-1} x_{l-2} \dots x_0} |1\rangle \right) = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i \cdot 0.x_0} |1\rangle \right) = \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i \cdot x_0 \cdot 2^{-1}} |1\rangle \right) = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{\pi i \cdot x_0} |1\rangle \right) = \begin{cases} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) & \text{si } x_0 = 0 \\ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) & \text{si } x_0 = 1 \end{cases} = \\ &= H |x_0\rangle \end{aligned}$$

En consecuencia, la QFT para $n = 1$ es precisamente la compuerta de Hadamard.

Circuito Cuántico de la QFT de 2-qubits

En este caso, $n=2$. Aplicando la Proposición 5.6, se tiene que si $x_0, x_1 \in \{0, 1\}$ entonces

$$QFT |x_1 x_0\rangle = \frac{1}{\sqrt{2^2}} \bigotimes_{l=1}^2 \left(|0\rangle + e^{2\pi i 0.x_{l-1}x_{l-2} \dots x_0} |1\rangle \right) =$$

$$\frac{1}{\sqrt{2^2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right)$$

Su circuito es el siguiente:

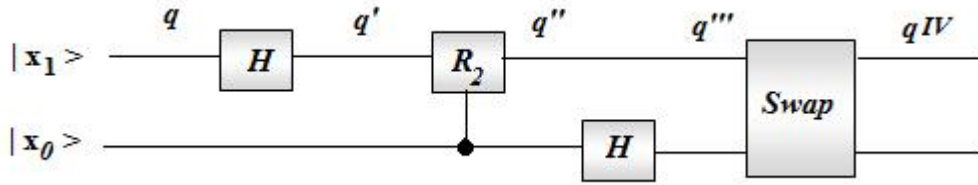


Figura 5.1: Circuito cuántico de la QFT para $n = 2$.

Se probará que efectivamente este circuito genera la Transformada Cuántica de Fourier sobre el espacio de 2-qubits.

Primeramente, el estado inicial del sistema es

$$q = |x_1\rangle \otimes |x_0\rangle$$

Los siguientes estados del sistema son:

$$q' = H |x_1\rangle \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_1} |1\rangle) \right) \otimes |x_0\rangle$$

Teniendo en cuenta que

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i x_0}{2^2}} \end{pmatrix}$$

Entonces

$$q'' = R_2 \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_1} |1\rangle) \right) \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} (R_2 |0\rangle + e^{2\pi i 0.x_1} R_2 |1\rangle) \right) \otimes |x_0\rangle =$$

$$= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1} e^{\frac{2\pi i x_0}{2^2}} |1\rangle \right) \right) \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_1} e^{2\pi i 0.0x_0} |1\rangle) \right) \otimes |x_0\rangle =$$

$$= \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i (0.x_1 + 0.0x_0)} |1\rangle) \right) \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle) \right) \otimes |x_0\rangle$$

El próximo paso consiste en aplicar la compuerta H al segundo qubit $|x_0\rangle$:

$$\begin{aligned}
q''' &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \otimes H |x_0\rangle = \\
&= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \right)
\end{aligned}$$

Finalmente, al aplicar la compuerta Swap se obtiene

$$\begin{aligned}
q^{IV} &= \text{Swap} \left(\left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \right) \right) = \\
&= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) = \\
&= \frac{1}{\sqrt{2^2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) = \\
&= \frac{1}{\sqrt{2^2}} \bigotimes_{l=1}^2 \left(|0\rangle + e^{2\pi i 0.x_{l-1} x_{l-2} \dots x_0} |1\rangle \right) = \text{QFT} |x_1 x_0\rangle
\end{aligned}$$

Circuito Cuántico de la QFT de 3-qubits

En este caso, $n=3$. Aplicando la Proposición 5.6, se tiene que si $x_0, x_1, x_2 \in \{0, 1\}$ entonces

$$\begin{aligned}
\text{QFT} |x_2 x_1 x_0\rangle &= \frac{1}{\sqrt{2^3}} \bigotimes_{l=1}^3 \left(|0\rangle + e^{2\pi i 0.x_{l-1} x_{l-2} \dots x_0} |1\rangle \right) = \\
&= \frac{1}{\sqrt{2^3}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right)
\end{aligned}$$

Su circuito es el siguiente:

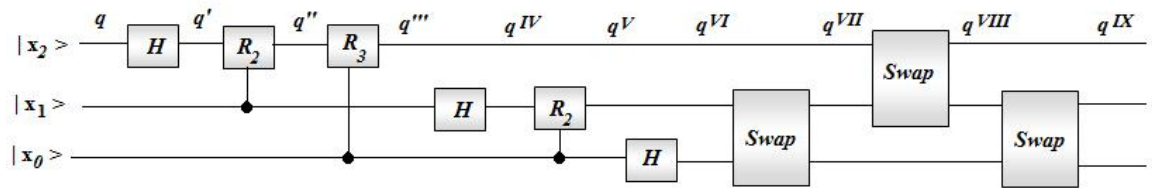


Figura 5.2: Circuito cuántico de la QFT para $n = 3$.

Nuevamente se probará que efectivamente este circuito genera la Transformada Cuántica de Fourier sobre el espacio de 3-qubits. Primeramente, el estado inicial del sistema es

$$q = |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle$$

Al aplicar la compuerta H al primer qubit se tiene:

$$q' = H |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2} |1\rangle \right) \right) \otimes |x_1\rangle \otimes |x_0\rangle$$

Como

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i x_1}{2^2}} \end{pmatrix}$$

Entonces

$$\begin{aligned} q'' &= R_2 \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_2} |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} (R_2 |0\rangle + e^{2\pi i 0.x_2} R_2 |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2} e^{\frac{2\pi i x_1}{2^2}} |1\rangle \right) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_2} e^{2\pi i 0.0x_1} |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i (0.x_2 + 0.0x_1)} |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_2x_1} |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle \end{aligned}$$

Al aplicar la compuerta

$$R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i x_0}{2^3}} \end{pmatrix}$$

Resulta

$$\begin{aligned} q''' &= R_3 \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_2x_1} |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} (R_3 |0\rangle + e^{2\pi i 0.x_2x_1} R_3 |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2x_1} e^{\frac{2\pi i x_0}{2^3}} |1\rangle \right) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_2x_1} e^{2\pi i 0.00x_0} |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_2x_1x_0} |1\rangle) \right) \otimes |x_1\rangle \otimes |x_0\rangle \end{aligned}$$

Al aplicar la compuerta H al segundo qubit se obtiene el siguiente estado

$$q^{IV} = \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0.x_2x_1x_0} |1\rangle) \right) \otimes H |x_1\rangle \otimes |x_0\rangle =$$

$$= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1} |1\rangle \right) \right) \otimes |x_0\rangle$$

A continuación se aplica al segundo qubit la compuerta

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i x_0}{2^2}} \end{pmatrix}$$

Con lo cual resulta el siguiente estado:

$$\begin{aligned} q^V &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes R_2 \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1} |1\rangle \right) \right) \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(R_2 |0\rangle + e^{2\pi i 0.x_1} R_2 |1\rangle \right) \right) \otimes |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \otimes |x_0\rangle \end{aligned}$$

Aplicando la compuerta H al tercer qubit resulta:

$$\begin{aligned} q^{VI} &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \otimes H |x_0\rangle = \\ &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \right) \end{aligned}$$

A continuación se intercambian el Segundo y tercer qubit a través de la compuerta Swap:

$$\begin{aligned} q^{VII} &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \text{Swap} \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \right) = \\ &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \end{aligned}$$

Luego se intercambian el primer y segundo qubit para obtener el siguiente estado:

$$\begin{aligned} q^{VIII} &= \text{Swap} \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) = \\ &= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle \right) \right) \otimes \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle \right) \right) \end{aligned}$$

Finalmente se intercambian el segundo y tercer qubit

$$\begin{aligned}
q^{IX} &= \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0x_0} |1\rangle) \right) \otimes \text{Swap} \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0x_2x_1x_0} |1\rangle) \right) \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0x_1x_0} |1\rangle) \right) = \\
&= \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0x_0} |1\rangle) \right) \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0x_1x_0} |1\rangle) \right) \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i 0x_2x_1x_0} |1\rangle) \right) = \\
&= \frac{1}{\sqrt{2^3}} \bigotimes_{l=1}^3 \left(|0\rangle + e^{2\pi i 0x_{l-1}x_{l-2}\dots x_0} |1\rangle \right) = \text{QFT} |x_2x_1x_0\rangle
\end{aligned}$$

Circuito Cuántico de la QFT de n-qubits (caso general)

El circuito cuántico que implementa la Transformada Cuántica de Fourier de n-qubits utiliza compuertas de Hadamard, de Desplazamiento de Fase y compuertas Swaps. Para simplificar su representación gráfica, se omitirán las compuertas Swaps. El circuito se muestra a continuación:

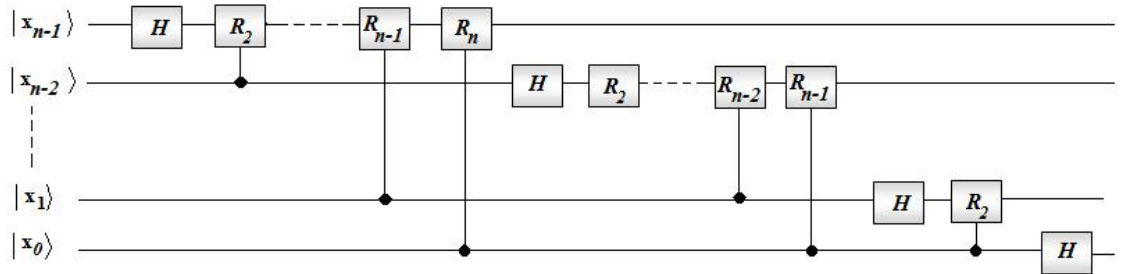


Figura 5.3: Circuito cuántico de la QFT de n qubits.

Como se puede comprobar, el qubit $|x_0\rangle$ requiere una compuerta de Hadamard, el qubit $|x_1\rangle$ requiere una compuerta de Hadamard y una de Desplazamiento de Fase y cada qubit que le antecede precisa una compuerta adicional de Desplazamiento de Fase. En la próxima sección se analizará el costo que demanda construir el circuito cuántico asociado a la Transformada Cuántica de Fourier, contando la cantidad de compuertas requeridas para su diseño.

Cantidad de compuertas requeridas para el circuito cuántico de la QFT de n-qubits

Primeramente se enunciará la siguiente Proposición, que determina la cantidad de compuertas Swaps utilizadas en el circuito cuántico de la Transformada Cuántica de Fourier.

Proposición 5.7

La cantidad de compuertas Swaps que se necesitan para transformar un n-qubit $|x_{n-1}x_{n-2}\dots x_1x_0\rangle$ en el n-qubit $|x_0x_1\dots x_{n-2}x_{n-1}\rangle$ es

$$\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}$$

Demostración

Será desarrollada por el tesista Ariel Savarese. ■

El siguiente cuadro muestra cuántas compuertas necesita cada qubit de entrada del circuito cuántico para la Transformada Cuántica de Fourier:

<i>Qubit de entrada</i>	<i>Cantidad de compuertas</i>
$ x_0\rangle$	<i>1 compuerta de Hadamard</i>
$ x_1\rangle$	<i>1 compuerta de Hadamard y 1 compuerta de Desplazamiento de Fase</i>
:	:
:	:
$ x_{n-2}\rangle$	<i>1 compuerta de Hadamard y (n-2) compuertas de Desplazamiento de Fase</i>
$ x_{n-1}\rangle$	<i>1 compuerta de Hadamard y (n-1) compuertas de Desplazamiento de Fase</i>

Por otro lado, según la Proposición 5.7, se requieren $\frac{n(n-1)}{2}$ compuertas Swaps. Por lo tanto, el total de compuertas necesarias para implementar el circuito cuántico es:

$$\begin{aligned}
 & n \text{ compuertas de Hadamard} + \sum_{i=1}^{n-1} i \text{ compuertas de Desplazamiento de Fase} + \\
 & \frac{n(n-1)}{2} \text{ compuertas Swaps} = \\
 & = n + \sum_{i=1}^{n-1} i + \frac{n(n-1)}{2} \text{ compuertas} = n + \frac{n(n-1)}{2} + \frac{n(n-1)}{2} \text{ compuertas} = \\
 & = n^2 \text{ compuertas.}
 \end{aligned}$$

En consecuencia, el circuito cuántico de la Transformada Cuántica de Fourier de n -qubits contiene $O(n^2)$ compuertas cuánticas. Si se compara con la Transformada Discreta de Fourier, se puede probar que ésta utiliza $O(n 2^n)$ compuertas lógicas, donde n es la cantidad de bits. Por esta razón se puede afirmar que la Transformada Cuántica de Fourier mejora exponencialmente a la Transformada Discreta de Fourier.

Capítulo 6

Aplicación de la Transformada Cuántica de Fourier

En este capítulo se mostrará cómo aplicar la Transformada Cuántica de Fourier para hallar el período de una función exponencial modular.

Esta aplicación es de suma importancia, pues desempeña un rol fundamental en el Algoritmo de Shor. De hecho, es la parte del algoritmo que consume la mayor parte del tiempo computacional.

Previamente se introducirán algunas definiciones y se demostrarán resultados matemáticos que serán utilizados para justificar el algoritmo cuántico que calcula el período de este tipo de funciones.

Definición 6.1: La función exponencial modular

Una función exponencial modular es una función $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_n$ de la forma

$$f(x) = a^x \pmod{n}$$

Donde $n \in \mathbb{N}$ y a es un elemento invertible en $\mathbb{Z}_n$. Es decir, $\text{mcd}(a, n) = 1$.

Definición 6.2: Función periódica en $\mathbb{Z}_n$

Una función $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_n$ es periódica si $\exists p \in \mathbb{N}$ tal que

$$f(x + p) = f(x) \quad \forall x \in \mathbb{Z}_{\geq 0}$$

En este caso, se dice que el período es

$$P = \min \{ p \in \mathbb{N} / f(x + p) = f(x) \quad \forall x \in \mathbb{Z}_{\geq 0} \}$$

La siguiente Proposición prueba que la exponencial modular es una función periódica e indica cuál es su período.

Proposición 6.3

La función exponencial modular $f(x) = a^x \pmod{n}$ es periódica, y su período es

$$P = \min \{ p \in \mathbb{N} / a^p \equiv 1 \pmod{n} \}$$

Además, $P < n$.

Demostración

Como a es invertible en $\mathbb{Z}_n$ entonces a^x es también invertible y su inverso es

$$(a^{-1})^x = a^{-x}.$$

Por lo tanto

$$f(x+p)=f(x) \Leftrightarrow a^{x+p}=a^x \Leftrightarrow a^x \cdot a^p=a^x \Leftrightarrow a^{-x} \cdot a^x \cdot a^p=a^{-x} \cdot a^x \Leftrightarrow 1 \cdot a^p=1 \Leftrightarrow a^p=1 \text{ en } \mathbb{Z}_n \Leftrightarrow a^p \equiv 1 \pmod{n}.$$

En consecuencia,

$$f(x+p)=f(x) \Leftrightarrow a^p \equiv 1 \pmod{n} \quad [1]$$

Luego

$$f(x) \text{ es periódica } \Leftrightarrow \exists p \in \mathbb{N} \text{ tal que } a^p \equiv 1 \pmod{n}.$$

Por la Proposición 1.56 incisos 2) y 4) se tiene que $\exists r \in \mathbb{N}$ con $r < n$ tal que

$$r = \min \left\{ k \in \mathbb{N} / a^k \equiv 1 \pmod{n} \right\}$$

Teniendo en cuenta [1], se toma $P = r$. De aquí resulta que $f(x)$ es periódica, de período P , con $P < n$. ■

A continuación se definirá la compuerta f asociada a una función exponencial modular. Esta compuerta será la encargada de guardar los valores de dicha función.

Definición 6.4: La compuerta f de la función exponencial modular

Sea $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_n$ definida por $f(x) = a^x \pmod{n}$, con $n \in \mathbb{N}$ y a un elemento invertible en $\mathbb{Z}_n$. Sea $m \in \mathbb{N}$ tal que $n \leq 2^m$. La compuerta f de $2m$ qubits, simbolizada por U_f , es la transformación lineal unitaria definida por

$$U_f(|x\rangle |y\rangle) = |x\rangle |y \oplus f(x)\rangle$$

Donde $x, y \in \mathbb{Z}_{2^m}$

$|x\rangle$ es la representación en base 10 del m -qubit $|x_{m-1} \ x_{m-2} \dots x_1 \ x_0\rangle$

$|y\rangle$ es la representación en base 10 del m -qubit $|y_{m-1} \ y_{m-2} \dots y_1 \ y_0\rangle$

$\oplus$ es la suma módulo 2 bit a bit.

El siguiente Ejemplo ilustrará cómo calcular dicha compuerta.

Ejemplo 6.5

Sea $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_4$ definida por $f(x) = 3^x \pmod{4}$. Sea U_f la compuerta f de 8 qubits. Calcular

a) $U_f(|0\rangle |1\rangle)$

b) $U_f(|1\rangle |2\rangle)$

c) $U_f(|2\rangle |3\rangle)$

Solución

En este caso, $m = n = 4$. Entonces

a)

$$U_f(|0\rangle |1\rangle) = |0\rangle |1 \oplus f(0)\rangle = |0\rangle |1 \oplus 1\rangle = |0\rangle |0001 \oplus 0001\rangle = |0\rangle |0000\rangle = |0\rangle |0\rangle$$

b)

$$U_f(|1\rangle|2\rangle) = |1\rangle|2 \oplus f(1)\rangle = |1\rangle|2 \oplus 3\rangle = |1\rangle|0010 \oplus 0011\rangle = |1\rangle|0001\rangle = |1\rangle|1\rangle$$

c)

$$U_f(|2\rangle|3\rangle) = |2\rangle|3 \oplus f(2)\rangle = |2\rangle|3 \oplus 1\rangle = |2\rangle|0011 \oplus 0001\rangle = |2\rangle|0010\rangle = |2\rangle|2\rangle$$

La siguiente Proposición muestra qué relación existe entre los puntos del dominio de una función exponencial modular que tienen la misma imagen.

Proposición 6.6

Sea $f(x) = a^x \pmod{n}$, con $n \in \mathbb{N}$ y a un elemento invertible en $\mathbb{Z}_n$. Sea P el período de $f(x)$ y $x, x_0 \in \mathbb{Z}_{\geq 0}$ tales que $x > x_0$. Entonces

$$f(x) = f(x_0) \pmod{n} \Leftrightarrow x = x_0 + j.P \text{ con } j \in \mathbb{N}.$$

Demostración

$\Leftarrow$) Sea $x = x_0 + j.P$ con $j \in \mathbb{N}$ y tal que $(x_0 + j.P) < n$. Entonces, como P es el período de $f(x)$ se tiene:

$$\begin{aligned} f(x) &= f(x_0 + j.P) = f(x_0 + (j-1).P + P) = f(x_0 + (j-1).P) = \\ &= f(x_0 + (j-2).P + P) = f(x_0 + (j-2).P) = \dots = f(x_0 + (j-(j-1)).P) = \\ &= f(x_0 + P) = f(x_0) \pmod{n}. \end{aligned}$$

$\Rightarrow$) Como a es invertible en $\mathbb{Z}_n$ entonces a^{x_0} es también invertible y su inverso es

$$(a^{-1})^{x_0} = a^{-x_0}.$$

Por lo tanto

$$\text{Como } f(x) = f(x_0) \Rightarrow a^x \equiv a^{x_0} \pmod{n} \Rightarrow a^x \cdot a^{-x_0} \equiv a^{x_0} \cdot a^{-x_0} \pmod{n}$$

Luego

$$a^{x-x_0} \equiv 1 \pmod{n} \quad [1]$$

En consecuencia, por la Proposición 6.3, resulta que $x - x_0 \geq P$. Por otro lado, por el Algoritmo de la División Entera, se tiene que

$$x - x_0 = j.P + r_1 \text{ con } j \in \mathbb{N} \text{ y } 0 \leq r_1 < P \quad [2]$$

Si se supone que $r_1 > 0$ entonces, reemplazando [2] en [1] y aplicando la Proposición 1.51 resulta

$$1 \equiv a^{x-x_0} \equiv a^{j.P+r_1} \equiv a^{j.P} \cdot a^{r_1} \equiv (a^P)^j \cdot a^{r_1} \equiv (1)^j \cdot a^{r_1} \equiv a^{r_1} \pmod{n}$$

Por lo tanto,

$$a^{r_1} \equiv 1 \pmod{n}$$

Lo cual es una contradicción pues, por la Proposición 6.3,

$$P = \min \{p \in \mathbb{N} / a^p \equiv 1 \pmod{n}\}$$

En consecuencia,

$$r_1 = 0 \quad [3]$$

Reemplazando [3] en [2] se obtiene finalmente que

$$x - x_0 = j.P$$

Es decir,

$$x = j.P + x_0 \quad \blacksquare$$

En la próxima sección se introducirá la noción de “fracción continua” y se mostrarán algunas de sus propiedades. Estos conceptos se utilizarán para determinar el período de una función exponencial modular.

Fracciones continuas

Definición 6.7: Fracción continua

Una fracción continua es una expresión de la forma

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots}}}}$$

Donde $a_0 \in \mathbb{Z} \wedge a_i \in \mathbb{N} \quad \forall i = 1, 2, \dots$

Notación 6.8: A una fracción continua x se la suele simbolizar por $x = [a_0, a_1, a_2, \dots]$

Definición 6.9: Convergentes de una fracción continua

Dada una fracción continua $x = [a_0, a_1, a_2, \dots]$, los convergentes de dicha fracción son

$$[a_0] = a_0$$

$$[a_0, a_1] = a_0 + \frac{1}{a_1}$$

$$[a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$$

En general, el k -ésimo convergente es

$$[a_0, a_1, a_2, \dots, a_k] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots a_{k-2} + \frac{1}{a_{k-1} + \frac{1}{a_k}}}}}}$$

Notación 6.10: Al k -ésimo convergente de una fracción continua, por ser un número racional, se lo simbolizará por

$$[a_0, a_1, a_2, \dots, a_k] = \frac{n_k}{d_k}$$

Cómo calcular una fracción continua

Para hallar la representación en fracción continua del número real x , se procede así:

Primer Paso: Se considera la parte entera de x , simbolizada por $[x]$.

Segundo Paso: Se calcula “la parte fraccionaria de x ”, es decir, $x - [x]$. Si la parte fraccionaria da 0, el proceso termina. En caso contrario se ejecuta el Tercer Paso.

Tercer Paso: Se calcula el “recíproco de la parte fraccionaria”, es decir, $\frac{1}{x - [x]}$.

Se vuelve al *Primer Paso*, reemplazando x por $\frac{1}{x - [x]}$.

El siguiente Ejemplo muestra cómo calcular la fracción continua de un número.

Ejemplo 6.11

Sea $x = 3.245$

- Calcular la fracción continua de x .
- Indicar todos los convergentes de la fracción continua de x .

Solución

- Se diseña el siguiente cuadro:

Paso	Número x	Parte entera de x	Parte fraccionaria de x	Recíproco Parte fraccionaria (f)	Expresión en fracción mixta de f
1	3.245	3	$0.245 = \frac{245}{1000}$	$\frac{1000}{245}$	$4 \frac{20}{245}$
2	$4 \frac{20}{245}$	4	$\frac{20}{245}$	$\frac{245}{20}$	$12 \frac{5}{20}$
3	$12 \frac{5}{20}$	12	$\frac{5}{20}$	$\frac{20}{5}$	4
4	4	4	0	Fin	

Por lo tanto $3.245 = [3, 4, 12, 4]$

- Los convergentes de la fracción continua de x son:

$$[3] = 3$$

$$\begin{aligned}
[3,4] &= 3 + \frac{1}{4} = \frac{13}{4} \\
[3,4,12] &= 3 + \frac{1}{4 + \frac{1}{12}} = \frac{159}{49} \\
[3,4,12,4] &= 3 + \frac{1}{4 + \frac{1}{12 + \frac{1}{4}}} = \frac{649}{200} = 3.245
\end{aligned}$$

Algunas propiedades de las fracciones continuas

En esta sección se enunciarán algunas propiedades de las funciones continuas que serán utilizadas en el algoritmo para determinar el período de una función exponencial modular.

Teorema 6.12

Los convergentes de una fracción continua son fracciones irreducibles. Es decir, si $x = [a_0, a_1, a_2, \dots]$ y si $[a_0, a_1, a_2, \dots, a_k] = \frac{n_k}{d_k}$ es el k -ésimo convergente entonces $\text{mcd}(n_k, d_k) = 1$.

Demostración

Véase [13].

Teorema 6.13

El desarrollo de una fracción continua de x es finito sii x es racional.

Demostración

Véase [13].

Teorema 6.14

Sean $n, y_0 \in \mathbb{N}$ y $\frac{p}{q}$ una fracción irreducible tal que

$$\left| \frac{y_0}{2^n} - \frac{p}{q} \right| < \frac{1}{(2)^{2^n}}$$

Entonces $\frac{p}{q} = \frac{n_k}{d_k}$ para algún k . Es decir, $\frac{p}{q}$ es un convergente de la fracción continua de $\frac{y_0}{2^n}$.

Demostración

Véase [13].

Proposición 6.15

Sean $n, y_0, k, r \in \mathbb{N}$ tales que $\frac{y_0}{2^n} = \frac{k}{r}$. Si $\frac{k}{r}$ es irreducible entonces

$$\frac{k}{r} = \frac{n_k}{d_k}$$

Para algún k , donde $\frac{n_k}{d_k}$ es el k -ésimo convergente de $\frac{y_0}{2^n}$.

Demostración

Se aplica el Teorema 6.14 con $\frac{p}{q} = \frac{k}{r}$. Entonces

$$\left| \frac{y_0}{2^n} - \frac{k}{r} \right| = 0 < \frac{1}{(2)^{2^n}}.$$

Por lo tanto $\frac{k}{r} = \frac{n_k}{d_k}$ para algún k , donde $\frac{n_k}{d_k}$ es el k -ésimo convergente de $\frac{y_0}{2^n}$. ■

Proposición 6.16

Sean $a, b, c, d \in \mathbb{N}$ tales que $\frac{a}{b} = \frac{c}{d}$ con $\frac{a}{b}$ y $\frac{c}{d}$ fracciones irreducibles. Entonces

$$a = c \wedge b = d$$

Demostración

Como $\frac{a}{b}$ y $\frac{c}{d}$ son fracciones irreducibles, entonces $\text{mcd}(a, b) = 1 \wedge \text{mcd}(c, d) = 1$.

Por lo tanto, por el Teorema 1.27, $\exists p, q, s, t \in \mathbb{N}$ tales que

$$\begin{cases} 1 = p.a + q.b \\ 1 = s.c + t.d \end{cases} \quad [1]$$

Por otro lado, como $\frac{a}{b} = \frac{c}{d}$ entonces

$$\begin{cases} a = \frac{b.c}{d} \\ c = \frac{a.d}{b} \end{cases} \quad [2]$$

Reemplazando la primera ecuación de [2] en la primera de [1] resulta $1 = p \cdot \frac{b.c}{d} + q.b$

Luego $d = (p.c + q.d) b$. De aquí resulta que

$$d \mid b \quad [3]$$

De manera similar, reemplazando la segunda ecuación de [2] en la segunda de [1] se obtiene

$$b \mid d \quad [4]$$

De [3] y [4] se tiene que $\exists k_1, k_2 \in \mathbb{N}$ tales que

$$\begin{cases} b = k_1 \cdot d \\ d = k_2 \cdot b \end{cases} \quad [5]$$

Multiplicando miembro a miembro las ecuaciones [5] se tiene

$$b \cdot d = k_1 \cdot k_2 \cdot b \cdot d \quad [6]$$

Como $b \cdot d \neq 0$ entonces de [6] resulta

$$1 = k_1 \cdot k_2$$

Como $k_1, k_2 \in \mathbb{N}$ entonces

$$k_1 = k_2 = 1 \quad [7]$$

Sustituyendo [7] en [5] se obtiene que

$$b = d \quad [8]$$

Finalmente, reemplazando [8] en [2] resulta

$$a = c \quad \blacksquare$$

Proposición 6.17

Sean $n, y_0, k, r \in \mathbb{N}$ tales que $\frac{y_0}{2^n} = \frac{k}{r}$, con $\frac{k}{r}$ fracción irreducible. Entonces r es igual al denominador de algún convergente de la fracción continua de $\frac{y_0}{2^n}$.

Demostración

Por la Proposición 6.15, $\frac{k}{r} = \frac{n_k}{d_k}$ para algún k . Por otro lado de la Proposición 6.16 resulta $r = d_k$. ■

En base a estas nociones matemáticas previas, se detallará a continuación el algoritmo cuántico que determina el período de una función exponencial modular.

Descripción del algoritmo cuántico para el cálculo del período de una función exponencial modular

Como se mencionó anteriormente, el algoritmo que se describirá a continuación calculará el período P de una función $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_n$ de la forma

$$f(x) = a^x \pmod{n}$$

Donde $n \in \mathbb{N}$ y a es un elemento invertible en $\mathbb{Z}_n$.

Primeramente se toma $m \in \mathbb{N}$ que verifique

$$n^2 \leq 2^m < 2n^2.$$

Es decir, se elige $m \in \mathbb{N}$ de modo tal que $2 \log_2(n) \leq m < 1 + 2 \log_2(n)$.

El algoritmo consta de dos partes:

Parte cuántica: Es ejecutada por una computadora cuántica. Es la encargada de obtener un m -qubit utilizando un determinado circuito cuántico.

Parte clásica: Es ejecutada por una computadora convencional. Se encarga de hallar, a partir de dicho m -qubit, posibles candidatos al período P y de chequear cuál de ellos es.

Los detalles de cada una de estas partes se muestran a continuación:

Parte cuántica

Se diseña un circuito cuántico que posea $2m$ entradas:

$$q_1 = q_2 = \dots = q_m = q_{m+1} = \dots = q_{2m} = |0\rangle$$

Los primeros m qubits forman el primer registro, mientras que los últimos m qubits constituyen el segundo registro del sistema.

La representación gráfica de dicho circuito es la siguiente:

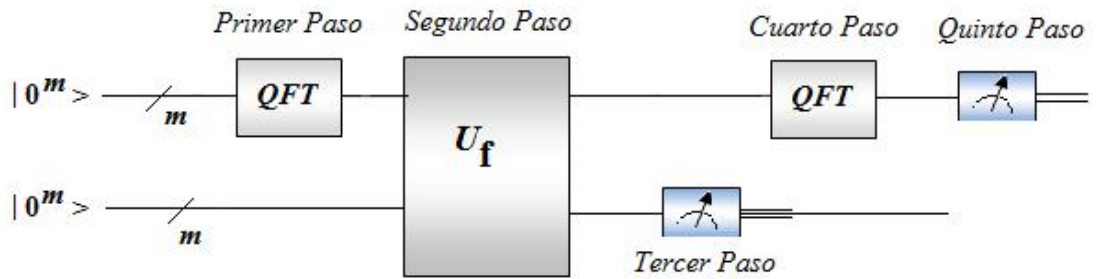


Figura 6.1: Circuito cuántico para el cálculo del período de una función exponencial modular.

En este caso, el estado inicial del sistema es

$$q = q_1 \otimes q_2 \otimes \dots \otimes q_m \otimes q_{m+1} \dots \otimes q_{2m} = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \dots \otimes |0\rangle = |0^m\rangle \otimes |0^m\rangle$$

Al expresar cada registro en base 10, el estado inicial se escribe

$$q = |0\rangle \otimes |0\rangle$$

Primer Paso

Se aplica la Transformada Cuántica de Fourier al primer registro. Luego, por la Proposición 3.11, el sistema evoluciona al siguiente estado:

$$q' = QFT |0\rangle \otimes |0\rangle = \left(\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle e^{\frac{2\pi i x \cdot 0}{2^m}} \right) \otimes |0\rangle = \frac{1}{\sqrt{2^m}} \left(\sum_{x=0}^{2^m-1} |x\rangle \otimes |0\rangle \right)$$

Es decir,

$$q' = \frac{1}{\sqrt{2^m}} \left(\sum_{x=0}^{2^m-1} |x\rangle |0\rangle \right)$$

Segundo Paso

Al atravesar la compuerta f de $2m$ qubits, el sistema evoluciona del siguiente modo:

$$\begin{aligned} q'' &= U_f q' = U_f \left(\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle |0\rangle \right) = \frac{1}{\sqrt{2^m}} \left(\sum_{x=0}^{2^m-1} U_f (|x\rangle |0\rangle) \right) = \\ &= \frac{1}{\sqrt{2^m}} \left(\sum_{x=0}^{2^m-1} |x\rangle \otimes |0 \oplus f(x)\rangle \right) = \frac{1}{\sqrt{2^m}} \left(\sum_{x=0}^{2^m-1} |x\rangle \otimes |f(x)\rangle \right) = \sum_{x=0}^{2^m-1} \frac{1}{\sqrt{2^m}} |x\rangle \otimes |f(x)\rangle \end{aligned}$$

Por lo tanto

$$q'' = \sum_{x=0}^{2^m-1} \frac{1}{\sqrt{2^m}} |x\rangle \otimes \underbrace{|f(x)\rangle}_{\text{Segundo registro.}}$$

De esta manera se ha obtenido en forma simultánea el valor de $f(x)$ para 2^m valores de x . Es aquí donde se pone de manifiesto el paralelismo cuántico.

Tercer Paso

Se efectúa la medición del segundo registro, es decir, de los m últimos qubits. En este caso, se obtendrá un m -qubit $|f(x_0)\rangle$, para algún $x_0 \in \{0, 1, \dots, 2^m - 1\}$.

Para determinar a qué estado colapsará el sistema, se analizarán qué puntos del dominio de f (restringido a $\mathbb{Z}_{2^m}$) tienen imagen igual a $f(x_0)$. Para ello, se definen

$$\begin{aligned} z_0 &= \min \left\{ x \in \{0, 1, \dots, 2^m - 1\} / f(x) = f(x_0) \right\} \\ A &= \left\{ x \in \{0, 1, \dots, 2^m - 1\} / f(x) = f(x_0) \right\} \end{aligned}$$

En consecuencia

$$A = \left\{ x \in \{0, 1, \dots, 2^m - 1\} / f(x) = f(z_0) \right\}$$

Entonces, de la Proposición 6.6 resulta

$$A = \left\{ x \in \{0, 1, \dots, 2^m - 1\} / x = z_0 + P \cdot j, \text{ con } j \in \mathbb{Z}_{\geq 0} \text{ tal que } (z_0 + P \cdot j) < 2^m \right\}$$

Como $j < \frac{2^m - z_0}{P}$ entonces

$$j \leq \left\lfloor \frac{2^m - z_0}{P} \right\rfloor$$

Donde $\lfloor x \rfloor$ es la parte entera del número x . Luego, si se define

$$M = \left\lfloor \frac{2^m - z_0}{P} \right\rfloor + 1$$

Resulta

$$A = \{z_0, z_0 + P, z_0 + 2P, \dots, z_0 + (M-1)P\}$$

Luego, por la Proposición 2.26 (generalizada a un sistema de $2m$ -qubits), el sistema colapsa al siguiente estado:

$$\begin{aligned} q''' &= \frac{\sum_{x \in A} \frac{1}{\sqrt{2^m}} |x\rangle |f(x_0)\rangle}{\sqrt{\underbrace{\left(\frac{1}{\sqrt{2^m}}\right)^2 + \left(\frac{1}{\sqrt{2^m}}\right)^2 + \dots + \left(\frac{1}{\sqrt{2^m}}\right)^2}_{\text{card}(A) \text{ veces}}} = \frac{\sum_{x \in A} \frac{1}{\sqrt{2^m}} |x\rangle |f(x_0)\rangle}{\sqrt{\text{card}(A)} \frac{1}{2^m}} = \\ &= \frac{\frac{1}{\sqrt{2^m}} \sum_{x \in A} |x\rangle |f(x_0)\rangle}{\sqrt{\text{card}(A)} \frac{1}{\sqrt{2^m}}} = \frac{\sum_{x \in A} |x\rangle |f(x_0)\rangle}{\sqrt{\text{card}(A)}} = \frac{\sum_{j=0}^{M-1} |z_0 + P \cdot j\rangle |f(x_0)\rangle}{\sqrt{M}} \end{aligned}$$

Es decir

$$q''' = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} \underbrace{|z_0 + P \cdot j\rangle}_{\text{Primer registro}} |f(x_0)\rangle$$

Primer registro.

Donde $M = \left\lfloor \frac{2^m - z_0}{P} \right\rfloor + 1$, $\text{card}(A)$: cantidad de elementos que tiene A .

Cuarto Paso

Se aplica la Transformada Cuántica de Fourier al primer registro. En este caso, el sistema evoluciona al siguiente estado:

$$\begin{aligned} q^{IV} &= \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} \text{QFT}(|z_0 + P \cdot j\rangle) |f(x_0)\rangle = \\ &= \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i (z_0 + P \cdot j)y}{2^m}} |y\rangle |f(x_0)\rangle = \\ &= \frac{1}{\sqrt{M 2^m}} \sum_{j=0}^{M-1} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i (z_0 + P \cdot j)y}{2^m}} |y\rangle |f(x_0)\rangle \end{aligned}$$

Es decir

$$q^{IV} = \frac{1}{\sqrt{M 2^m}} \sum_{j=0}^{M-1} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i (z_0 + P \cdot j)y}{2^m}} |y\rangle |f(x_0)\rangle$$


 Primer registro.

Quinto Paso

Se efectúa la medición del primer registro, es decir, de los primeros m qubits. Así, se obtendrá un m -qubit $|y_0\rangle$, para algún $y_0 \in \{0, 1, \dots, 2^m - 1\}$.

Parte clásica

Se tratará de hallar el período P a partir del m -qubit $|y_0\rangle$ que se observó. Como se verá, en dicho m -qubit estarán “escondidos” los posibles candidatos a ser P .

Primeramente se analizará qué m -qubit $|y_0\rangle$ tiene más chance de salir al efectuar la medición. Es decir, se calculará

$$\text{Prob}(y = y_0) \quad \forall y_0 \in \{0, 1, \dots, 2^m - 1\}.$$

Para hallar tal probabilidad, se debe tener en cuenta que los términos del estado q^{IV} cuyo valor de “ y ” es igual a y_0 son

$$\frac{1}{\sqrt{M 2^m}} \sum_{j=0}^{M-1} e^{\frac{2\pi i (z_0 + P \cdot j)y_0}{2^m}} |y_0\rangle |f(x_0)\rangle = \left(\frac{1}{\sqrt{M 2^m}} \sum_{j=0}^{M-1} e^{\frac{2\pi i (z_0 + P \cdot j)y_0}{2^m}} \right) |y_0\rangle |f(x_0)\rangle$$

Teniendo en cuenta el Tercer Postulado de la Mecánica Cuántica (confrontar las Definiciones 2.4 y 2.9), la probabilidad de encontrar el primer registro del sistema en estado y_0 es:

$$\begin{aligned} \text{Prob}(y = y_0) &= \left| \frac{1}{\sqrt{M 2^m}} \sum_{j=0}^{M-1} e^{\frac{2\pi i (z_0 + P \cdot j)y_0}{2^m}} \right|^2 = \left| \frac{1}{\sqrt{M 2^m}} \right|^2 \cdot \left| \sum_{j=0}^{M-1} e^{\frac{2\pi i (z_0 + P \cdot j)y_0}{2^m}} \right|^2 = \\ &= \left| \frac{1}{\sqrt{M 2^m}} \right|^2 \cdot \left| \sum_{j=0}^{M-1} e^{\frac{2\pi i (z_0 + P \cdot j)y_0}{2^m}} \right|^2 = \frac{1}{M 2^m} \underbrace{\left| e^{\frac{2\pi i z_0 y_0}{2^m}} \right|^2}_{=1} \left| \sum_{j=0}^{M-1} e^{\frac{2\pi i P \cdot j y_0}{2^m}} \right|^2 \end{aligned}$$

Por la Fórmula de Euler

Por lo tanto

$$\text{Prob}(y = y_0) = \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} e^{\frac{2\pi i P \cdot j y_0}{2^m}} \right|^2 \quad [1]$$

Obsérvese que, por la desigualdad triangular, se tiene que

$$\begin{aligned} \text{Prob}(y = y_0) &= \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} e^{\frac{2 \pi i P \cdot j y_0}{2^m}} \right|^2 \leq \frac{1}{M 2^m} \left(\sum_{j=0}^{M-1} \left| e^{\frac{2 \pi i P \cdot j y_0}{2^m}} \right| \right)^2 = \\ &= \frac{1}{M 2^m} \left(\sum_{j=0}^{M-1} 1 \right)^2 = \frac{1}{M 2^m} \cdot M^2 = \frac{M}{2^m} \end{aligned}$$

Es decir,

$$\text{Prob}(y = y_0) \leq \frac{M}{2^m} \quad \forall y_0 \in \{0, 1, \dots, 2^m - 1\}$$

Esta cota superior de la probabilidad es alcanzada si $e^{\frac{2 \pi i P y_0}{2^m}} = 1$ pues

$$\begin{aligned} \text{Prob}(y = y_0) &= \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} e^{\frac{2 \pi i P \cdot j y_0}{2^m}} \right|^2 = \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} \left(e^{\frac{2 \pi i P \cdot y_0}{2^m}} \right)^j \right|^2 = \\ &= \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} (1)^j \right|^2 = \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} 1 \right|^2 = \frac{M^2}{M 2^m} = \frac{M}{2^m} \end{aligned}$$

Al aplicar la igualdad de números complejos expresados en forma exponencial resulta

$$\begin{aligned} e^{\frac{2 \pi i P y_0}{2^m}} = 1 &\Leftrightarrow e^{\frac{2 \pi i P y_0}{2^m}} = 1 \cdot e^{i \cdot 0} \Leftrightarrow \frac{2 \pi P y_0}{2^m} = 0 + 2k\pi \Leftrightarrow \frac{y_0 P}{2^m} = \frac{k}{P} \text{ con } k \in \mathbb{Z} \\ &\Leftrightarrow \frac{y_0 P}{2^m} \in \mathbb{Z} \end{aligned}$$

Por lo tanto

$$e^{\frac{2 \pi i P y_0}{2^m}} = 1 \Leftrightarrow \frac{y_0 P}{2^m} \in \mathbb{Z}$$

En consecuencia, si existe $y_0 \in \{0, 1, \dots, 2^m - 1\}$ que verifique:

$$\frac{y_0 P}{2^m} \in \mathbb{Z}$$

Entonces el m -qubit $|y_0\rangle$ es el que tiene más chance de salir.

Pero ¿qué sucede si ningún y_0 verifica que $\frac{y_0 P}{2^m} \in \mathbb{Z}$? A pesar de que en la práctica es

imposible chequear si $\frac{y_0 P}{2^m}$ es o no un número entero (pues en esta expresión figura el

período P , cuyo valor es desconocido), esta expresión brinda suficiente información para encontrar el período P . Por esta razón se considerarán dos casos:

Primer Caso: Existe $y_0 \in \{0, 1, \dots, 2^m - 1\}$ tal que $\frac{y_0 P}{2^m} \in \mathbb{Z}$

En este caso,

$$\frac{y_0}{2^m} = \frac{k}{P} \text{ para algún } k \in \mathbb{Z}. \quad [2]$$

Como se vio recientemente, cualquier y_0 que verifique esta condición será el que tendrá más probabilidad de salir. Además, $\frac{k}{P}$ se puede expresar en términos de una fracción irreducible simplificando los factores comunes a k y a P . Es decir,

$$\frac{k}{P} = \frac{k_1}{P_1} \quad [3]$$

Donde $k_1, P_1, k_2 \in \mathbb{N}$ son tales que

$$k = k_1 \cdot k_2, P = P_1 \cdot k_2 \wedge \text{mcd}(k_1, P_1) = 1$$

Luego, de [2] y [3] resulta

$$\frac{y_0}{2^m} = \frac{k_1}{P_1}$$

Con $\frac{k_1}{P_1}$ fracción irreducible. Por la Proposición 6.17, P_1 es igual al denominador de

algún convergente de la fracción continua de $\frac{y_0}{2^m}$. Es decir,

$$d = P_1 \quad [4]$$

Donde

d : es el denominador de un convergente de la fracción continua de $\frac{y_0}{2^m}$.

Multiplicando en ambos miembros de la ecuación [4] por k_2 resulta

$$d \cdot k_2 = P_1 \cdot k_2$$

Por lo tanto

$$d \cdot k_2 = P \text{ con } k_2 \in \mathbb{N} \quad [5]$$

De la ecuación [5] se deduce que el período P es un múltiplo del denominador de un convergente de la fracción continua de $\frac{y_0}{2^m}$.

En consecuencia, los posibles candidatos a ser el período P son:

$$d \cdot k_2$$

Con $k_2 \in \mathbb{N}$ y tal que $d \cdot k_2 < n$

Para hallar P basta chequear, aplicando el Algoritmo para el Cálculo de la Potencia Modular descrito en el Capítulo 1, cuál de ellos verifica que $a^{d \cdot k_2} \equiv 1 \pmod{n}$.

Segundo Caso: $\frac{y_0 P}{2^m} \notin \mathbb{Z} \quad \forall y_0 \in \{0, 1, \dots, 2^m - 1\}$

En este caso, dado $y_0 \in \{0, 1, \dots, 2^m - 1\}$, si se efectúa la división entera de $y_0 P$ por 2^m , resulta

$$y_0 P = q_0 \cdot 2^m + r_0$$

Donde $q_0, r_0 \in \mathbb{Z}$ y tal que $1 \leq r_0 < 2^m$

Por lo tanto

$$\frac{y_0}{2^m} - \frac{q_0}{P} = \frac{r_0}{P \cdot 2^m}$$

Como r_0 y P son números positivos entonces

$$\left| \frac{y_0}{2^m} - \frac{q_0}{P} \right| = \frac{r_0}{P \cdot 2^m} \quad [6]$$

Se puede probar (véase [5], pág. 678) que $\text{Prob}(y = y_0)$ es máxima cuando $r_0 < \frac{P}{2}$.

Por lo tanto, de la ecuación [6] resulta

$$\left| \frac{y_0}{2^m} - \frac{q_0}{P} \right| = \frac{r_0}{P \cdot 2^m} < \frac{\frac{P}{2}}{P \cdot 2^m} = \frac{1}{(2) 2^m}$$

Es decir,

$$\left| \frac{y_0}{2^m} - \frac{q_0}{P} \right| < \frac{1}{(2) 2^m} \quad [7]$$

Nuevamente, como se hizo en el Primer Caso, se expresa $\frac{q_0}{P}$ en términos de una fracción irreducible, simplificando los factores comunes a q_0 y a P . De este modo

$$\frac{q_0}{P} = \frac{k_1}{P_1} \quad [8]$$

Donde $k_1, P_1, k_2 \in \mathbb{N}$ son tales que $q_0 = k_1 \cdot k_2$, $P = P_1 \cdot k_2 \wedge \text{mcd}(k_1, P_1) = 1$

Sustituyendo [8] en [7] se obtiene

$$\left| \frac{y_0}{2^m} - \frac{k_1}{P_1} \right| < \frac{1}{(2) 2^m}$$

Del Teorema 6.14 se deduce que $\frac{k_1}{P_1}$ es un convergente de la fracción continua de

$\frac{y_0}{2^m}$. Luego, por el Teorema 6.12 y la Proposición 6.16, P_1 es igual al denominador de dicho convergente. Siguiendo el mismo razonamiento utilizado para el Primer Caso, se concluye que los posibles candidatos a ser el período P son:

$$d \cdot k_2$$

Donde

d : es el denominador de un convergente de la fracción continua de $\frac{y_0}{2^m}$.

$k_2 \in \mathbb{N}$ y tal que $d \cdot k_2 < n$

Cabe destacar que tanto el cálculo de los convergentes como el de la potencia modular se realizan en una computadora convencional.

Lo anteriormente expuesto permite elaborar el siguiente algoritmo para determinar el período P .

Algoritmo de búsqueda del período P de una función $f(x) = a^x \pmod{n}$

Parte Cuántica

1) Ejecutar los Pasos 1 al 5.

Parte Clásica

2) Si $y_0 = 0$ entonces
Volver al inciso 1)
Sino

Calcular los convergentes de la fracción continua de $\frac{y_0}{2^m}$

3) Tomar como candidatos al período P a expresiones de la forma:

$$d \cdot k$$

Donde

d : es el denominador de un convergente de la fracción continua de $\frac{y_0}{2^m}$

$k \in \mathbb{N}$ tal que $d \cdot k < n$

4) Chequear cuál de estos valores $d \cdot k$ resulta ser el período, verificando si
$$a^{d \cdot k} \equiv 1 \pmod{n}$$

Si ninguno resulta ser el período, volver al inciso 1).

El siguiente Ejemplo ilustra cómo hallar el período P .

Ejemplo 6.18

Sea $f(x) = 5^x \pmod{8}$. Se desea hallar su período P .

- Hallar el valor de m que indica el algoritmo cuántico descrito anteriormente.
- Al ejecutar el Quinto Paso del algoritmo, se tomó la medición de los primeros m qubits del sistema, obteniendo el m -qubit $|y_0\rangle = |24\rangle$. Calcular el período P .

Solución

a) En este caso, según lo especificado en el algoritmo cuántico, $n = 8$. Como m es tal que $n^2 \leq 2^m < 2n^2$ entonces $64 \leq 2^m < 128$.
Es decir,

$$\log_2(64) \leq m < \log_2(128) \Rightarrow 6 \leq m < 7.$$

Por lo tanto $m = 6$.

b) Se calculará primeramente la fracción continua del número

$$x = \frac{y_0}{2^m} = \frac{24}{2^6} = \frac{24}{64} = 0.375$$

Para ello se diseña el siguiente cuadro:

<i>Paso</i>	<i>Número x</i>	<i>Parte entera de x</i>	<i>Parte fraccionaria de x</i>	<i>Recíproco Parte fraccionaria (f)</i>	<i>Expresión en fracción mixta de f</i>
1	$\frac{24}{64} = 0.375$	0	$0.375 = \frac{24}{64}$	$\frac{64}{24}$	$2 \frac{2}{3}$
2	$2 \frac{2}{3}$	2	$\frac{2}{3}$	$\frac{3}{2}$	$1 \frac{1}{2}$
3	$1 \frac{1}{2}$	1	$\frac{1}{2}$	$\frac{2}{1}$	2
4	2	2	0	Fin	

Por lo tanto $0.375 = [0, 2, 1, 2]$

A continuación se calculan los convergentes de la fracción continua de $\frac{y_0}{2^m} = 0.375$:

$$[0] = 0$$

$$[0, 2] = 0 + \frac{1}{2} = \frac{1}{2}$$

$$[0, 2, 1] = 0 + \frac{1}{2 + \frac{1}{1}} = \frac{1}{3}$$

$$[0, 2, 1, 2] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}} = \frac{3}{8}$$

Luego, los convergentes son: $0, \frac{1}{2}, \frac{1}{3}, \frac{3}{8}$

Los denominadores de estos convergentes no nulos son 2, 3, 8.

Obsérvese que el denominador del convergente $[0]$ no se tiene en cuenta pues no aporta ninguna información, ya que puede ser cualquier número no nulo.

De este modo, los posibles candidatos a ser el período P son:

$$2k, 3k, 8k$$

Con $k \in \mathbb{N}$ y tal que $2k < n \wedge 3k < n \wedge 8k < n$. Es decir, tal que

$$2k < 8 \wedge 3k < 8 \wedge 8k < 8$$

Por lo tanto, los candidatos a ser el período P son: 2, 4, 6, 3.

Como $5^2 = 25 \equiv 1 \pmod{8}$ entonces, por la Proposición 6.3, el período de $f(x)$ es $P = 2$.

La siguiente Proposición muestra otra forma de expresar $Prob(y = y_0)$.

Proposición 6.19

$$\text{Si } Prob(y = y_0) = \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} e^{\frac{2 \pi i P \cdot j y_0}{2^m}} \right|^2 \text{ para } y_0 \in \{0, 1, \dots, 2^m - 1\} \wedge P, M \in \mathbb{N}$$

Entonces

$$Prob(y = y_0) = \begin{cases} \frac{M}{2^m} & \text{si } \frac{y_0 P}{2^m} \in \mathbb{Z} \\ \frac{1}{M 2^m} \frac{1 - \cos\left(\frac{\pi P y_0 M}{2^{m-1}}\right)}{1 - \cos\left(\frac{\pi P y_0}{2^{m-1}}\right)} & \text{si } \frac{y_0 P}{2^m} \notin \mathbb{Z} \end{cases}$$

Demostración

Sea $y_0 \in \{0, 1, \dots, 2^m - 1\}$. Entonces

Si $\frac{y_0 P}{2^m} \in \mathbb{Z}$, se comprueba fácilmente que $e^{\frac{2 \pi i P y_0}{2^m}} = 1$. Por lo tanto

$$\begin{aligned} Prob(y = y_0) &= \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} e^{\frac{2 \pi i P \cdot j y_0}{2^m}} \right|^2 = \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} \left(e^{\frac{2 \pi i P \cdot y_0}{2^m}} \right)^j \right|^2 = \\ &= \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} (1)^j \right|^2 = \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} 1 \right|^2 = \frac{M^2}{M 2^m} = \frac{M}{2^m} \end{aligned}$$

En consecuencia, si $\frac{y_0}{2^m} = \frac{k}{P}$ con $k \in \mathbb{Z}$ se obtiene

$$Prob(y = y_0) = \frac{M}{2^m} \quad [1]$$

Por otro lado, si $\frac{y_0 P}{2^m} \notin \mathbb{Z}$ entonces $e^{\frac{2 \pi i P y_0}{2^m}} \neq 1$. Luego

$$Prob(y = y_0) = \frac{1}{M 2^m} \left| \sum_{j=0}^{M-1} e^{\frac{2 \pi i P j y_0}{2^m}} \right|^2 = \frac{1}{M 2^m} \left| \underbrace{\sum_{j=0}^{M-1} \left(e^{\frac{2 \pi i P y_0}{2^m}} \right)^j}_{\text{Suma geométrica}} \right|^2 =$$

$$\begin{aligned}
&= \frac{1}{M 2^m} \left| \frac{1 - \left(e^{\frac{2 \pi i P y_0}{2^m}} \right)^M}{1 - e^{\frac{2 \pi i P y_0}{2^m}}} \right|^2 = \frac{1}{M 2^m} \left| \frac{1 - e^{\frac{2 \pi i P y_0 M}{2^m}}}{1 - e^{\frac{2 \pi i P y_0}{2^m}}} \right|^2 = \\
&= \frac{1}{M 2^m} \frac{\left| 1 - e^{\frac{2 \pi i P y_0 M}{2^m}} \right|^2}{\left| 1 - e^{\frac{2 \pi i P y_0}{2^m}} \right|^2} = \frac{1}{M 2^m} \frac{\left| 1 - \cos\left(\frac{2 \pi P y_0 M}{2^m}\right) - i \sin\left(\frac{2 \pi P y_0 M}{2^m}\right) \right|^2}{\left| 1 - \cos\left(\frac{2 \pi P y_0}{2^m}\right) - i \sin\left(\frac{2 \pi P y_0}{2^m}\right) \right|^2} = \\
&= \frac{1}{M 2^m} \frac{\left(1 - \cos\left(\frac{2 \pi P y_0 M}{2^m}\right) \right)^2 + \sin^2\left(\frac{2 \pi P y_0 M}{2^m}\right)}{\left(1 - \cos\left(\frac{2 \pi P y_0}{2^m}\right) \right)^2 + \sin^2\left(\frac{2 \pi P y_0}{2^m}\right)} = \\
&= \frac{1}{M 2^m} \frac{2 - 2 \cos\left(\frac{2 \pi P y_0 M}{2^m}\right)}{2 - 2 \cos\left(\frac{2 \pi P y_0}{2^m}\right)} = \frac{1}{M 2^m} \frac{1 - \cos\left(\frac{\pi P y_0 M}{2^{m-1}}\right)}{1 - \cos\left(\frac{\pi P y_0}{2^{m-1}}\right)}
\end{aligned}$$

Por lo tanto, si $\frac{y_0 P}{2^m} \notin \mathbb{Z}$ se obtiene

$$\text{Prob}(y = y_0) = \frac{1}{M 2^m} \frac{1 - \cos\left(\frac{\pi P y_0 M}{2^{m-1}}\right)}{1 - \cos\left(\frac{\pi P y_0}{2^{m-1}}\right)} \quad [2]$$

De [1] y [2] resulta

$$\text{Prob}(y = y_0) = \begin{cases} \frac{M}{2^m} & \text{si } \frac{y_0 P}{2^m} \in \mathbb{Z} \\ \frac{1}{M 2^m} \frac{1 - \cos\left(\frac{\pi P y_0 M}{2^{m-1}}\right)}{1 - \cos\left(\frac{\pi P y_0}{2^{m-1}}\right)} & \text{si } \frac{y_0 P}{2^m} \notin \mathbb{Z} \end{cases} \quad \blacksquare$$

El siguiente Ejemplo muestra cómo calcular la probabilidad de obtener un determinado m -qubit al efectuar la medición del primer o segundo registro del circuito cuántico detallado en este capítulo.

Si bien en la práctica esta probabilidad es imposible de hallar en forma exacta, el Ejemplo sirve para corroborar que efectivamente se puede obtener el período P a partir del m -qubit que resultó al efectuar la medición.

Ejemplo 6.20

Sea $f(x) = 2^x \pmod{5}$

- Hallar el valor de m que indica el algoritmo cuántico.
- Calcular $f(x)$ para $x \in \mathbb{Z}_{2^m}$.
- Al ejecutar el *Tercer Paso* del algoritmo, ¿qué m -qubit tiene mayor probabilidad de salir al efectuar la medición del segundo registro?
- Suponga que, una vez ejecutado el *Tercer Paso* del algoritmo, se obtuvo el m -qubit $|f(x_0)\rangle = |2\rangle$. Al ejecutar el *Quinto Paso* del algoritmo, ¿qué m -qubit $|y_0\rangle$ tiene mayor probabilidad de salir?
- De acuerdo al resultado obtenido en el inciso anterior, si se selecciona un m -qubit $|y_0\rangle$ que tiene mayor probabilidad de salir, ¿es posible obtener el período P a partir de dicho m -qubit?

Solución

- En este caso $n = 5$. De acuerdo a lo indicado en el algoritmo cuántico, el número $m \in \mathbb{N}$ debe verificar

$$n^2 \leq 2^m < 2n^2.$$

Es decir,

$$25 \leq 2^m < 50$$

Por lo tanto, $m = 5$.

- Se elabora la siguiente tabla, que contiene los valores de $f(x)$ para $x \in \mathbb{Z}_{2^5}$:

x	$f(x)$	x	$f(x)$	x	$f(x)$
0	1	12	1	24	1
1	2	13	2	25	2
2	4	14	4	26	4
3	3	15	3	27	3
4	1	16	1	28	1
5	2	17	2	29	2
6	4	18	4	30	4
7	3	19	3	31	3
8	1	20	1		
9	2	21	2		
10	4	22	4		
11	3	23	3		

Cabe destacar que estos valores funcionales son desconocidos por el usuario, ya que se encuentran “escondidos” en la compuerta U_f .

c) Antes de efectuar la medición del segundo registro, el estado del sistema es

$$q'' = \sum_{x=0}^{2^m-1} \frac{1}{\sqrt{2^m}} |x\rangle \otimes \underbrace{|f(x)\rangle}_{\text{Segundo registro.}}$$

Al medir el segundo registro del sistema, se obtiene un m -qubit $|f(x_0)\rangle$. Por lo tanto, por la Definición 2.9 (generalizada a $2m$ -qubits), la probabilidad de hallar el segundo registro en estado $|f(x_0)\rangle$ es

$$\text{Prob}(f(x) = f(x_0)) = \sum_{x \in I_f(x_0)} \left| \frac{1}{\sqrt{2^m}} \right|^2 = \sum_{x \in I_f(x_0)} \frac{1}{2^m} = \frac{1}{2^m} \cdot \text{card}(I_f(x_0))$$

Donde

$$I_f(x_0) = \left\{ x \in \{0, 1, \dots, 2^m - 1\} / f(x) = f(x_0) \right\}$$

$\text{card}(I_f(x_0))$: Cantidad de elementos que tiene el conjunto $I_f(x_0)$.

Observando la tabla del inciso b), se tiene que $f(x_0) \in \{1, 2, 3, 4\}$. Por lo tanto,

$f(x_0)$	$I_f(x_0)$	$\text{card}(I_f(x_0))$	$\text{Prob}(f(x) = f(x_0))$
1	$\{0, 4, 8, 12, 16, 20, 24, 28\}$	8	$\frac{8}{2^m}$
2	$\{1, 5, 9, 13, 17, 21, 25, 29\}$	8	$\frac{8}{2^m}$
3	$\{3, 7, 11, 15, 19, 23, 27, 31\}$	8	$\frac{8}{2^m}$
4	$\{2, 6, 10, 14, 18, 22, 26, 30\}$	8	$\frac{8}{2^m}$

En consecuencia, al medir el m -qubit correspondiente al segundo registro del sistema, aquéllos que pueden aparecer, y todos ellos con probabilidad $\frac{8}{2^m} = \frac{8}{2^5} = 0.25$, son

$$\begin{aligned} |1\rangle &= |00001\rangle \\ |2\rangle &= |00010\rangle \\ |3\rangle &= |00011\rangle \\ |4\rangle &= |00100\rangle \end{aligned}$$

d) Al medir el primer registro del sistema, se obtiene un m -qubit $|y_0\rangle$. Luego, de la Proposición 6.19, la probabilidad hallar el primer registro en estado $|y_0\rangle$ es

$$Prob(y = y_0) = \begin{cases} \frac{M}{2^m} & \text{si } \frac{y_0 P}{2^m} \in \mathbb{Z} \\ \frac{1}{M 2^m} \frac{1 - \cos\left(\frac{\pi P y_0 M}{2^{m-1}}\right)}{1 - \cos\left(\frac{\pi P y_0}{2^{m-1}}\right)} & \text{si } \frac{y_0 P}{2^m} \notin \mathbb{Z} \end{cases}$$

Observando la tabla del inciso b) se tiene:

$$z_0 = \min \left\{ x \in \{0, 1, \dots, 2^m - 1\} / f(x) = f(x_0) \right\} = \min \left\{ x \in \{0, 1, \dots, 31\} / f(x) = 2 \right\} = 1$$

$$P = 4$$

$$M = \left\lceil \frac{2^m - z_0}{P} \right\rceil = \left\lceil \frac{32 - 1}{4} \right\rceil + 1 = \lceil 7.5 \rceil + 1 = 7 + 1 = 8$$

$$\frac{M}{2^m} = \frac{8}{2^5} = 0.25$$

Reemplazando estos datos en la expresión de la probabilidad resulta

$$Prob(y = y_0) = \begin{cases} 0.25 & \text{si } \frac{y_0 4}{32} \in \mathbb{Z} \\ \frac{1}{8(32)} \frac{1 - \cos\left(\frac{\pi 4 y_0 8}{16}\right)}{1 - \cos\left(\frac{\pi 4 y_0}{16}\right)} & \text{si } \frac{y_0 4}{32} \notin \mathbb{Z} \end{cases} =$$

$$= \begin{cases} 0.25 & \text{si } \frac{y_0}{8} \in \mathbb{Z} \\ \frac{1}{8(32)} \frac{1 - \cos\left(\frac{2\pi y_0}{4}\right)}{1 - \cos\left(\frac{\pi y_0}{4}\right)} & \text{si } \frac{y_0}{8} \notin \mathbb{Z} \end{cases} = \begin{cases} 0.25 & \text{si } \frac{y_0}{8} \in \mathbb{Z} \\ 0 & \text{si } \frac{y_0}{8} \notin \mathbb{Z} \end{cases}$$

En base a estos datos, se elabora la siguiente tabla:

y_0	$Prob(y = y_0)$	y_0	$Prob(y = y_0)$	y_0	$Prob(y = y_0)$
0	0.25	12	0	24	0.25
1	0	13	0	25	0
2	0	14	0	26	0
3	0	15	0	27	0
4	0	16	0.25	28	0
5	0	17	0	29	0
6	0	18	0	30	0
7	0	19	0	31	0
8	0.25	20	0		
9	0	21	0		
10	0	22	0		
11	0	23	0		

En consecuencia, al medir el m -qubit correspondiente al primer registro del sistema, aquéllos que pueden aparecer, y todos ellos con probabilidad 0.25 , son

$$|0\rangle = |00000\rangle$$

$$|8\rangle = |01000\rangle$$

$$|16\rangle = |10000\rangle$$

$$|24\rangle = |11000\rangle$$

e) Se supondrá que, al ejecutar el *Quinto Paso* del algoritmo y efectuar la medición del primer registro, se obtuvo el m -qubit $|y_0\rangle = |16\rangle$. Se verá que, efectivamente, a partir de dicho m -qubit se puede obtener el período P . Primeramente se calculará la fracción continua del número

$$x = \frac{y_0}{2^m} = \frac{16}{2^5} = \frac{16}{32} = 0.5$$

Para ello se diseña el siguiente cuadro:

<i>Paso</i>	<i>Número x</i>	<i>Parte entera de x</i>	<i>Parte fraccionaria de x</i>	<i>Recíproco Parte fraccionaria (f)</i>	<i>Expresión en fracción mixta de f</i>
1	$\frac{16}{32} = 0.5$	0	$0.5 = \frac{1}{2}$	2	2
2	2	2	0	Fin	

Por lo tanto $0.5 = [0, 2]$

A continuación se calculan los convergentes de la fracción continua de $\frac{y_0}{2^m} = 0.5$:

$$[0] = 0$$

$$[0, 2] = 0 + \frac{1}{2} = \frac{1}{2}$$

Luego, los convergentes son: $0, \frac{1}{2}$

Los denominadores de estos convergentes no nulos son: 2.

De este modo, los posibles candidatos a ser el período P son:

$$2k$$

Con $k \in \mathbb{N}$ y tal que $2k < n$. Es decir, tal que

$$2k < 5$$

Por lo tanto, los candidatos a ser el período P son: 2, 4.

Como $2^4 = 16 \equiv 1 \pmod{5}$ entonces, por la Proposición 6.3, el período de $f(x)$ es $P = 4$.

Se finaliza este capítulo con un ejemplo que ilustra cómo se ejecuta, paso a paso, el algoritmo cuántico que calcula el período de una función exponencial modular.

Ejemplo 6.21

Sea $f : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_5$ definida por $f(x) = 3^x \pmod{5}$.

Aplicar el algoritmo cuántico para hallar el período de $f(x)$.

Solución

En este caso, $n = 5$. Primeramente se toma $m \in \mathbb{N}$ tal que $n^2 \leq 2^m < 2n^2$.

Por lo tanto, $m = 5$. De este modo, el circuito cuántico que implementa el algoritmo tendrá dos registros de 5 qubits cada uno, inicializados en estado 0. De este modo, el estado inicial del sistema será

$$q = |00000\rangle \otimes |00000\rangle$$

Expresando cada registro en base 10 resulta

$$q = |0\rangle \otimes |0\rangle$$

Primer Paso

Se aplica la Transformada Cuántica de Fourier al primer registro. Luego, el sistema evoluciona al siguiente estado:

$$q' = \frac{1}{\sqrt{2^m}} \left(\sum_{x=0}^{2^m-1} |x\rangle |0\rangle \right)$$

Segundo Paso

Al atravesar la compuerta f de $2m$ qubits, el sistema evoluciona del siguiente modo:

$$q'' = \sum_{x=0}^{2^m-1} \frac{1}{\sqrt{2^m}} |x\rangle \otimes \underbrace{|f(x)\rangle}_{\text{Segundo registro.}}$$

Tercer Paso

Se efectúa la medición del segundo registro, es decir, de los m últimos qubits. En este caso, se obtendrá un m -qubit $|f(x_0)\rangle$, para algún $x_0 \in \{0, 1, \dots, 2^m - 1\}$. Se supondrá que

$$|f(x_0)\rangle = |3\rangle$$

Obsérvese que, al efectuar la medición, $f(x_0)$ se conoce, pero se desconoce x_0 .

Luego, el sistema evoluciona al siguiente estado:

$$q''' = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} \underbrace{|z_0 + P \cdot j\rangle}_{\text{Primer registro.}} |f(x_0)\rangle$$

Donde

$$z_0 = \min \left\{ x \in \{0, 1, \dots, 2^m - 1\} / f(x) = f(x_0) \right\} = \min \left\{ x \in \{0, 1, \dots, 31\} / f(x) = 3 \right\}$$

P : periodo de $f(x)$

$$M = \left\lceil \frac{2^m - z_0}{P} \right\rceil + 1$$

Cuarto Paso

Se aplica la Transformada Cuántica de Fourier al primer registro. En este caso, el sistema evoluciona al siguiente estado:

$$q^{IV} = \frac{1}{\sqrt{M 2^m}} \sum_{j=0}^{M-1} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i (z_0 + P \cdot j)y}{2^m}} \underbrace{|y\rangle}_{\text{Primer registro.}} |f(x_0)\rangle$$

Quinto Paso

Se efectúa la medición del primer registro, es decir, de los primeros m qubits. Así, se obtendrá un m -qubit $|y_0\rangle$, para algún $y_0 \in \{0, 1, \dots, 2^m - 1\}$. Se supondrá que

$$|y_0\rangle = |8\rangle$$

Para hallar el período P , se calculará primeramente la fracción continua del número $x = \frac{y_0}{2^m} = \frac{8}{2^5} = 0.25$. Para ello se diseña el siguiente cuadro:

Paso	Número x	Parte entera de x	Parte fraccionaria de x	Recíproco Parte fraccionaria (f)	Expresión en fracción mixta de f
1	$\frac{8}{32} = 0.25$	0	$0.25 = \frac{25}{100}$	$\frac{100}{25}$	4
2	4	4	0	Fin	

Por lo tanto $0.25 = [0, 4]$

A continuación se calculan los convergentes de la fracción continua de $\frac{y_0}{2^m} = 0.25$:

$$[0] = 0$$

$$[0, 4] = 0 + \frac{1}{4} = \frac{1}{4}$$

Luego, los convergentes son: $0, \frac{1}{4}$

El denominador del único convergente no nulo es: 4.

De este modo, los posibles candidatos a ser el período P son:

$$4k$$

Con $k \in \mathbb{N}$ y tal que $4k < n$. Es decir, tal que

$$4k < 5$$

Por lo tanto, el único candidato a ser P es: 4.

Como $3^4 = 81 \equiv 1 \pmod{5}$ entonces, por la Proposición 6.3, el período de $f(x)$ es $P = 4$.

Capítulo 7

El Algoritmo de Shor

Uno de los problemas más desafiantes para los matemáticos consiste en hallar la descomposición de un número natural como producto de factores primos. Se sabe que esta descomposición existe gracias al Teorema Fundamental de la Aritmética, enunciado en el Capítulo 1, que afirma lo siguiente:

Todo número natural n mayor que 1 puede ser representado de una manera única, salvo el orden, como producto de potencias de números primos. Es decir,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i}$$

Donde

$p_1 < p_2 < \dots < p_k$ son primos $\wedge \alpha_i \in \mathbb{N}$

Este Teorema fue demostrado por primera vez de forma completa en 1801 por Carl Friedrich Gauss. De este modo, desde el punto de vista teórico, el Teorema asegura que dicha descomposición existe, pero ¿cómo hallarla en la práctica, cuando el número natural n es muy grande? La realidad es que no se conoce ningún algoritmo, aplicable en una computadora clásica, que resuelva eficientemente este problema. De hecho, un reciente intento por descomponer un número natural de 200 dígitos consumió más de medio siglo de tiempo de cálculo.

Esta gran dificultad en hallar tal descomposición fue aprovechada por los sistemas criptográficos, cuya seguridad se basa en la imposibilidad de descubrir, en un tiempo relativamente corto, la expresión de una clave numérica n como producto de factores primos.

Sin embargo, en 1995 Peter Shor desarrolló un algoritmo cuántico, llamado *El Algoritmo de Shor*. El mismo consiste en hallar un divisor de un número natural n . De esta manera, ejecutando sucesivas veces el algoritmo, se logra hallar la descomposición de n como producto de factores primos. Teóricamente, el tiempo que se tarda en hallar la descomposición es considerablemente menor al de un ordenador convencional.

Este algoritmo fue comprobado empíricamente por primera vez en 2001 por un grupo de IBM, que descompuso el número $n = 15$ en sus factores 3 y 5, utilizando una computadora cuántica de 7 qubits.

En este capítulo se detallará paso a paso el *Algoritmo de Shor*, mostrando además su correspondiente justificación matemática.

Presentación del problema

El problema que intenta solucionar el Algoritmo de Shor es el siguiente:

Dado un número natural $n > 1$, encontrar un número natural d entre 1 y n que divida a n .

Hipótesis requeridas para aplicar el Algoritmo de Shor

1) Se supone que el número natural n es impar, porque si fuera par, el problema está solucionado tomando $d = 2$.

2) Se supone que n no es potencia de ningún número primo. Es decir, si a es un número primo entonces $n \neq a^k \quad \forall k \in \mathbb{N}$.

Porque si $n = a^k$ para algún primo a y para algún $k \in \mathbb{N}$, el problema también estaría resuelto considerando $d = a$. Por lo tanto, por la Proposición 1.59, se supondrá que

$$n = p \cdot q$$

Con $p \wedge q$ coprimos.

Para chequear que $n \neq a^k \quad \forall k \in \mathbb{N} \wedge \forall a$ primo basta verificar, según el Corolario 1.62, que

$$\sqrt[k]{n} \notin \mathbb{N} \quad \forall k \in \mathbb{N} \text{ con } k \leq \log_2(n)$$

Esta comprobación se puede llevar a cabo utilizando una computadora clásica.

Descripción del Algoritmo de Shor

El algoritmo utiliza una computadora cuántica y una convencional. Los detalles se muestran a continuación:

Primer Paso

Se elige aleatoriamente un número natural a tal que $1 < a < n$.

Segundo Paso

Se calcula $\text{mcd}(a, n)$.

Para hallarlo se aplica el Algoritmo de Euclides (véase Capítulo 1), implementándolo en una computadora clásica.

Tercer Paso

Si $\text{mcd}(a, n) \neq 1$ entonces

Se toma $d = \text{mcd}(a, n)$ y el proceso termina.

Sino

Se considera la función $f(x) = a^x \pmod{n}$ y se calcula su período P .

Para hallar dicho período se utiliza el algoritmo cuántico descrito en el Capítulo 6.

Cuarto Paso

Si P es impar entonces

Se vuelve al *Primer Paso*.

Sino

Si $a^{\frac{P}{2}} \equiv -1 \pmod{n}$ o equivalentemente, si $a^{\frac{P}{2}} \equiv n-1 \pmod{n}$ entonces

Se vuelve al *Primer Paso*. La verificación de esta congruencia se lleva a cabo mediante una computadora convencional, aplicando el Algoritmo de Cálculo de una Potencia Modular, visto en el Capítulo 1.

Quinto Paso

Los factores no triviales del número n son $\gcd\left(a^{\frac{P}{2}}+1, n\right) \wedge \gcd\left(a^{\frac{P}{2}}-1, n\right)$ y el

proceso termina. El cálculo de estos máximos comunes divisores se realiza en una computadora clásica, aplicando nuevamente el Algoritmo de Euclides.

Justificación matemática del Algoritmo de Shor

En el *Primer* y *Segundo Paso* del algoritmo se elige aleatoriamente un número natural a tal que $1 < a < n$ y se calcula $\gcd(a, n)$.

Tercer Paso

Si $\gcd(a, n) \neq 1$, el proceso termina ya que el $\gcd(a, n)$ es un divisor no trivial de n .

Si $\gcd(a, n) = 1$, por el Teorema 1.41 resulta que a es invertible en $\mathbb{Z}_n$.

En este caso, se calcula el período P de la función $f(x) = a^x \pmod{n}$.

De la Proposición 6.3 se tiene que

$$P = \min \left\{ x \in \mathbb{N} / a^x \equiv 1 \pmod{n} \right\}$$

Con lo cual, de acuerdo a la Definición 1.55, P es también el orden de a .

Cuarto Paso

Se trata de hallar un elemento a invertible en $\mathbb{Z}_n$, de orden par P y tal que

$$a^{\frac{P}{2}} \not\equiv -1 \pmod{n}$$

La existencia de tal elemento $a \in \mathbb{Z}_n$ queda asegurada por el Teorema 1.60.

Quinto Paso

El elemento $a \in \mathbb{Z}_n$ que se encontró es invertible, de orden par P y verifica:

$$\begin{cases} a^P \equiv 1 \pmod{n} & [1] \\ a^{\frac{P}{2}} \not\equiv -1 \pmod{n} & [2] \end{cases}$$

Se probará que $\gcd\left(a^{\frac{P}{2}}+1, n\right) \wedge \gcd\left(a^{\frac{P}{2}}-1, n\right)$ son efectivamente factores no triviales del número n .

Primeramente, se observa que de la ecuación [1] se tiene

$$a^P - 1 \equiv 0 \pmod{n}$$

Como P es par entonces $\frac{P}{2} \in \mathbb{N}$. Por lo tanto esta última ecuación se puede expresar como

$$\left(a^{\frac{P}{2}}-1\right)\left(a^{\frac{P}{2}}+1\right) \equiv 0 \pmod{n} \quad [3]$$

Por otro lado

$$n \nmid \left(a^{\frac{P}{2}}-1\right) \quad [4]$$

Pues si se supone por el absurdo que $n \mid \left(a^{\frac{P}{2}}-1\right)$ entonces $a^{\frac{P}{2}} \equiv 1 \pmod{n}$ lo cual es una contradicción pues $P = \min \left\{ p \in \mathbb{N} / a^p \equiv 1 \pmod{n} \right\}$.

Además,

$$n \nmid \left(a^{\frac{P}{2}}+1\right) \quad [5]$$

Pues si se supone nuevamente por el absurdo que $n \mid \left(a^{\frac{P}{2}}+1\right)$ entonces $a^{\frac{P}{2}} \equiv -1 \pmod{n}$ lo cual es una contradicción por [2]. A continuación se probará que

$$\gcd\left(a^{\frac{P}{2}}+1, n\right) \neq 1 \wedge \gcd\left(a^{\frac{P}{2}}-1, n\right) \neq 1$$

A fin de simplificar la notación, se define

$$\begin{cases} u = a^{\frac{P}{2}}+1 \\ v = a^{\frac{P}{2}}-1 \end{cases}$$

Reemplazando estas expresiones en [3] se obtiene

$$u \cdot v \equiv 0 \pmod{n}$$

Es decir

$$u \cdot v = k \cdot n \text{ para algún } k \in \mathbb{Z} \quad [6]$$

Si se supone por el absurdo que $\text{mcd}(u, n) = 1$ entonces, por el Teorema 1.27, existen $s, t \in \mathbb{Z}$ tales que

$$s \cdot u + t \cdot n = 1 \quad [7]$$

Al multiplicar miembro a miembro la ecuación [7] por v y aplicando la ecuación [6] se tiene

$$s \cdot u \cdot v + t \cdot n \cdot v = v \Rightarrow s \cdot k \cdot n + t \cdot n \cdot v = v \Rightarrow (s \cdot k + t \cdot v) \cdot n = v.$$

Por lo tanto

$$n \mid v$$

Es decir

$$n \mid \left(\frac{P}{a^2} - 1 \right)$$

Pero esto es una contradicción por [4]. De manera similar se prueba que $\text{mcd}(v, n) \neq 1$.

En consecuencia, $\text{mcd}\left(\frac{P}{a^2} + 1, n\right) \wedge \text{mcd}\left(\frac{P}{a^2} - 1, n\right)$ son factores no triviales de n .

Observación 7.1

1) La parte más costosa del Algoritmo de Shor es el *Tercer Paso*, pues el cálculo del período de una función exponencial modular demanda muchísimo tiempo de cómputo si se llevara a cabo en una computadora clásica. Sin embargo, si se utiliza una computadora cuántica y se aplica la Transformada Cuántica de Fourier, el tiempo de cálculo del período se reduce drásticamente, gracias a la propiedad del Paralelismo Cuántico que poseen las partículas subatómicas. Es allí donde radica la genialidad del algoritmo.

2) Por otro lado, cabe preguntarse lo siguiente:

¿Cuántas veces habrá que repetir el algoritmo hasta encontrar el número “ a ” conveniente?

Se puede probar que el algoritmo debe repetirse $O(\log(\log(n)))$ veces hasta hallar dicho “ a ”. La demostración de este resultado escapa al objetivo de este trabajo.

3) También se puede demostrar que el Algoritmo de Shor tarda un tiempo $O((\log(n))^3)$ en descomponer en factores primos el número n . Por esta razón se dice

que su orden de complejidad es polinomial. A modo de comparación, uno de los mejores algoritmos clásicos de factorización es el Algoritmo de Pollard y Strassen,

creado en 1976. Su orden de complejidad es $O\left(2^{\frac{m}{4}} \cdot m^2\right)$ donde m es la cantidad de

dígitos del número n . Esto prueba que el Algoritmo de Shor resuelve el problema de factorización en un tiempo considerablemente menor al de cualquier otro algoritmo conocido hasta ahora.

En la siguiente sección se desarrollarán dos Ejemplos que ilustrarán la forma de implementar el Algoritmo de Shor.

Ejemplo 7.2

Aplicar el Algoritmo de Shor para hallar la descomposición del número $n = 15$ como producto de factores primos.

Solución

Primero Paso

Se elige aleatoriamente un número natural a tal que $1 < a < 15$. Por ejemplo, se toma $a = 13$.

Segundo Paso

Se calcula $\text{mcd}(a, n) = \text{mcd}(13, 15) = 1$.

Tercer Paso

Como $\text{mcd}(13, 15) = 1$, se considera la función $f(x) = 13^x \pmod{15}$ y se calcula su período P . Es decir, se busca

$$P = \min \left\{ x \in \mathbb{N} / 13^x \equiv 1 \pmod{15} \right\}$$

Se obtiene que $P = 4$.

Cuarto Paso

Como P es par se calcula $a^{\frac{P}{2}} = 13^{\frac{4}{2}} = 13^2 = 169 \equiv 4 \pmod{15}$

Se verifica que $a^{\frac{P}{2}} \not\equiv -1 \pmod{15}$ pues $4 \not\equiv -1 \pmod{15}$.

O equivalentemente, de la Proposición 1.30 inciso 9), porque $4 \not\equiv 15 - 1 = 14 \pmod{15}$

Quinto Paso

Los factores no triviales del número $n=15$ son $\text{mcd}\left(a^{\frac{P}{2}} + 1, n\right) \wedge \text{mcd}\left(a^{\frac{P}{2}} - 1, n\right)$.

Es decir,

$$\text{mcd}\left(a^{\frac{P}{2}} + 1, n\right) = \text{mcd}\left(13^2 + 1, 15\right) = \text{mcd}(170, 15) = 5$$

$$\text{mcd}\left(a^{\frac{P}{2}} - 1, n\right) = \text{mcd}\left(13^2 - 1, 15\right) = \text{mcd}(168, 15) = 3$$

Por lo tanto, 5 y 3 son factores de $n = 15$.

Como $15 = (5)(3)$, la factorización de 15 como producto de números primos fue hallada.

Ejemplo 7.3

Sea $n = 1617$.

- 1) Aplicar el Algoritmo de Shor para hallar dos divisores de n .
- 2) Hallar la descomposición de n como producto de factores primos.

Solución

1) Primero Paso

Se elige aleatoriamente un número natural a tal que $1 < a < 1617$. Por ejemplo, se toma $a = 50$.

Segundo Paso

Se calcula $\text{mcd}(a, n) = \text{mcd}(50, 1617) = 1$.

Tercer Paso

Como $\text{mcd}(50, 1617) = 1$, se considera la función $f(x) = 50^x \pmod{1617}$ y se calcula su período P . Es decir, se busca

$$P = \min \left\{ x \in \mathbb{N} / 50^x \equiv 1 \pmod{1617} \right\}$$

Aplicando el algoritmo cuántico detallado en el Capítulo 6, Se obtiene que $P = 10$.

Cuarto Paso

Como P es par se calcula $a^{\frac{P}{2}} = 50^{\frac{10}{2}} = 50^5 \equiv 197 \pmod{1617}$

Se verifica que $a^{\frac{P}{2}} \not\equiv -1 \pmod{1617}$ pues $197 \not\equiv -1 \pmod{1617}$.

Quinto Paso

Los factores no triviales del número $n=1617$ son $\text{mcd}\left(a^{\frac{P}{2}} + 1, n\right) \wedge \text{mcd}\left(a^{\frac{P}{2}} - 1, n\right)$.

Es decir,

$$\text{mcd}\left(a^{\frac{P}{2}} + 1, n\right) = \text{mcd}\left(50^5 + 1, 1617\right) = 33$$

$$\text{mcd}\left(a^{\frac{P}{2}} - 1, n\right) = \text{mcd}\left(50^5 - 1, 1617\right) = 49$$

Por lo tanto, 33 y 49 son factores de $n = 1617$.

2) Para hallar la descomposición de n como producto de factores primos, se buscarán otros posibles factores de 1617. Para ello se aplica nuevamente el Algoritmo de Shor al número que resulta de dividir 1617 por alguno de sus divisores hallados. Es decir, se aplica el Algoritmo de Shor a

$$\frac{1617}{33} \text{ o bien a } \frac{1617}{49}.$$

Como $\frac{1617}{33} = 49 = 7^2$ es potencia de un número primo, el Algoritmo de Shor no puede aplicarse a dicho número. Pero $\frac{1617}{49} = 33$ no es potencia de un número primo. Por lo tanto, se aplicará el algoritmo al número 33. Es decir que, en este caso, $n = 33$.

Primero Paso

Se elige aleatoriamente un número natural a tal que $1 < a < 33$. Por ejemplo, se toma $a = 10$.

Segundo Paso

Se calcula $\text{mcd}(a, n) = \text{mcd}(10, 33) = 1$.

Tercer Paso

Como $\text{mcd}(10, 33) = 1$, se considera la función $f(x) = 10^x \pmod{33}$ y se calcula su período P . Es decir, se busca

$$P = \min \left\{ x \in \mathbb{N} / 10^x \equiv 1 \pmod{33} \right\}$$

Se obtiene que $P = 2$.

Cuarto Paso

Como P es par se calcula $a^{\frac{P}{2}} = 10^{\frac{2}{2}} = 10 \pmod{33}$

Se verifica que $a^{\frac{P}{2}} \neq -1 \pmod{33}$ pues $10 \neq -1 \pmod{33}$.

O equivalentemente, porque $10 \neq 33 - 1 = 32 \pmod{33}$

Quinto Paso

Los factores no triviales del número $n=33$ son $\text{mcd}\left(a^{\frac{P}{2}} + 1, n\right) \wedge \text{mcd}\left(a^{\frac{P}{2}} - 1, n\right)$.

Es decir,

$$\text{mcd}\left(a^{\frac{P}{2}} + 1, n\right) = \text{mcd}\left(10^1 + 1, 33\right) = \text{mcd}(11, 33) = 11$$

$$\text{mcd}\left(a^{\frac{P}{2}} - 1, n\right) = \text{mcd}\left(10^1 - 1, 33\right) = \text{mcd}(9, 33) = 3$$

Por lo tanto, 11 y 3 son divisores primos de $n = 33$. Así,

$$33 = (11) \cdot (3)$$

Como $\frac{1617}{49} = 33 \Rightarrow 1617 = (49) \cdot (33) = (49) \cdot (11) \cdot (3) = (7^2) \cdot (11) \cdot (3)$

De este modo, la descomposición de 1617 como producto de factores primos es

$$1617 = (7^2) \cdot (11) \cdot (3)$$

Lenguajes de programación para computadoras cuánticas

Uno de los lenguajes de programación para una computadora cuántica es el qGCL. La explicación de cada una de sus sentencias y reglas específicas para ejecutarlas figura en [16]. A modo de ejemplo, en la siguiente Figura se muestra el código fuente del Algoritmo de Shor, escrito en dicho lenguaje.

```
For natural numbers  $x$  and  $y$ , we write  $x \sqcup y$  for their maximum and  $gcd(x, y)$ 
for their greatest-common divisor. Shor's algorithm is

var  $t : \mathbb{B}$ ,  $a, d, p : 0 \dots (n+1)$  •
   $t := 0$ 
do  $\neg t$ 
   $a := 2 \dots n$ 
   $d := gcd(a, n)$ 
  if  $d \neq 1$      $t := 1$ 
  []  $d = 1$      $Q(a, n; p)$ 
               if  $p$  odd     $t := 1$ 
               []  $p$  even
                $d := gcd(a^{p/2}-1, n) \sqcup gcd(a^{p/2}+1, n)$ 
                $t := (d \neq 1)$ 
               fi
  fi
od
```

Figura 7.1: Código fuente del Algoritmo de Shor, escrito en lenguaje qGCL.

Vulnerabilidad del sistema criptográfico RSA ante el Algoritmo de Shor

El sistema criptográfico **RSA** (desarrollado en 1979 en el MIT por sus creadores **R**ivest, **S**hamir y **A**dleman) es uno de los algoritmos más utilizados para cifrar mensajes, emitir claves bancarias y firmar digitalmente. Contiene una clave para encriptar, que es pública, y otra para desencriptar, que es privada.

Estas claves contienen un número natural n gigantesco (de 200 o más dígitos) y que se expresa como producto de dos números primos. Es decir,

$$n = p \cdot q$$

Donde $p \wedge q$ son primos.

El número n se conoce, pero se desconocen p y q . Descubriendo cuáles son estos dos últimos números, el mensaje puede descifrarse fácilmente.

La seguridad de este algoritmo radica en que, si se utiliza una computadora tradicional, no hay maneras rápidas de expresar un número muy grande como producto de factores primos.

Sin embargo, la computación cuántica puede proveer una solución a este problema de factorización gracias al Algoritmo de Shor.

Por esta razón se prevé que en un futuro próximo las computadoras cuánticas harán vulnerables numerosos algoritmos criptográficos y, en particular, el tan difundido sistema **RSA**.

Capítulo 8

Conclusiones

El Algoritmo Cuántico de Shor resuelve el problema de factorización de un número natural en un tiempo considerablemente menor al de cualquier otro algoritmo que se implemente en una computadora clásica.

Más específicamente, resuelve este problema en tiempo polinomial, mientras que otros algoritmos lo resuelven en tiempo exponencial.

Su aporte innovador radica en el uso de la Transformada Cuántica de Fourier para calcular el período de una función exponencial modular. Gracias a ello, el Algoritmo de Shor se torna sumamente eficiente.

En este sentido, cabe mencionar el pensamiento del Prof. Jesús Soto (Universidad Católica de Murcia), quien en su artículo de la página web citada en [14], manifestó:

“El Algoritmo de Shor ha pasado a ser considerado un paradigma de los algoritmos cuánticos y su fama, en cierta medida, se debe al trasfondo de su utilización. Así por ejemplo, la descomposición en factores primos es la clave para atacar al RSA y otros sistemas criptográficos mundialmente utilizados.

Además, pone de manifiesto que la venidera era de los computadores cuánticos dejará obsoletos los actuales sistemas criptográficos”.

Por otro lado, el presente trabajo de tesis brinda un enfoque matemático, con demostraciones detalladas de las propiedades que se aplican, paso a paso, en los algoritmos cuánticos desarrollados.

El rigor matemático utilizado facilitará el entendimiento del funcionamiento de otros algoritmos y circuitos cuánticos.

Por último, en relación a los desafíos planteados al inicio de esta tesis, se considera la meta cumplida, ya que se incorporaron numerosos ejemplos que facilitarán al lector la comprensión de los temas.

Referencias

- [1] Peter W. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM J.Sci.Statist.Comput, 1997.
- [2] <https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17>
- [3] Oviedo, Pablo Andrés. “*Fundamentos Matemáticos de Computación Cuántica en el Algoritmo de Shor, para la factorización prima de números enteros*”. Tesis de Licenciatura en Matemática. Directora: Abdel Masih, Samira. Universidad Abierta Interamericana. Buenos Aires, 2017.
- [4] Prieto, Cecilia Andrea. “*Modelo compacto del algoritmo Diffie-Hellman utilizando cuaterniones*”. Tesis de Licenciatura en Matemática. Directora: Abdel Masih, Samira. Universidad Abierta Interamericana. Buenos Aires, 2019.
- [5] Loceff, Michael. “*A course of Quantum Computing, Volume 1*”. Ed. Los Altos Hills, California, 2015.
- [6] Nielsen, Michael & Chuang, Isaac. “*Quantum Computation and Quantum Information*”. Cambridge University Press, 2016.
- [7] McMahon, David Isaac. “*Quantum Computation Explained*”. John Wiley & Sons, 2008.
- [8] <http://www.fisicafundamental.net/misterios/computacion.html#introduccion>
- [9] D. Deutch and R. Jozsa. “*Rapid solution of problems by quantum computation*”. *Proc. Roy Soc. London Ser.* pp 553-558, 1992
- [10] Chris Bernhardt. “*Quantum Computing for everyone*”. MIT Press pp 157-167, 2019.
- [11] Granado Peralta, S. “*Matemática Discreta*”. Ed. CEIT. Buenos Aires, 2002.
- [12] https://es.wikipedia.org/wiki/Teorema_chino_del_resto
- [13] N. Beskin. “*Fracciones Maravillosas*”. Ed. MIR. Moscú, 1987.
- [14] <http://pimedios.es/2015/04/23/el-qubit-y-el-algoritmo-de-shor/>
- [15] Laverde Alfonso, Sebastián. “*Estudio comparativo y Evaluación de utilidad de protocolos de transmisión de datos usando Criptografía Cuántica, pág. 16-18*”. Trabajo de grado para optar al título de Ingeniero Electrónico. Director: González Jiménez, Edgar. Pontificia Universidad javeriana. Bogotá, 2016.
- [16] J.W. Sanders and P. Zuliani. “*Quantum Programming*”. Oxford University Computing Laboratory. England. 2018.